1. Scopo e Campo di applicazione

2. Documenti

3. Definizioni

4. Requisiti specifici per la certificazione Security Manager

5. Criteri per la certificazione Iniziale

6. Sorveglianza, mantenimento, rinnovo della certificazione ed estensione delle competenze. Passaggio da altro ODC

7. Sospensione e revoca della Certificazione

8. Reclami e Ricorsi

9. Uso del Logo

10 Codice Deontologico

REDAZIONE Responsabile di Schema	Data 21.09.26
VERIFICA Responsabile Tecnico	Data 21.09.26
APPROVAZIONE Amministratore Unico	Data 21.09.26

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Regolamento ha lo scopo di definire i requisiti minimi per la certificazione delle competenze, il mantenimento ed il rinnovo della citata certificazione, delle figure dei Security Manager. La norma applicabile, è la UNI 10459:2017 – Professionista della Security.

2. DOCUMENTI

- **UNI CEI EN ISO/IEC 17024:2012** – Valutazione della conformità –Requisiti generali per gli organismi operanti la certificazione delle persone.
- **RG - 01 – ACCREDIA** (per la parte di competenza) Regolamento per l'Accreditamento degli Organismi di Certificazione, Ispezione, Verifica e Convalida – Parte Generale.
- **RG – 01 – 02 – ACCREDIA**: Regolamento per l'Accreditamento degli Organismi di Certificazione del Personale

GUIDA CEN 14:2010 Linee guida di indirizzo per le attività di normazione sulla qualificazione delle professioni e del personale

- **Raccomandazione del Parlamento Europeo e del Consiglio 2009/C 155/02 del 18.06.2009** sull'istituzione di Un Sistema Europeo di Crediti per l'istruzione e la formazione professionale (ECVET)
- **Raccomandazione del Parlamento Europeo e del Consiglio del 23.04.2008,** sulla costituzione del quadro europeo delle qualifiche per l'apprendimento permanente (EFQ)
- **Decreto Legislativo 16.01.2013 n° 13** – Definizione delle norme generali e dei livelli essenziali delle prestazioni per l'individuazione e validazione degli apprendimenti non formali e informali e degli standard minimi di servizio del sistema nazionale di certificazione delle competenze, a norma dell'articolo 4, commi 58 e 68, della legge 28 giugno 2012, n. 92
- **Legge 04/2013**: Disposizioni in materia di professioni non organizzate.
- **Decreto Ministero dell'Interno 01.12.2010 n° 269 e s.m.i.** "Regolamento recante disciplina delle caratteristiche minime del Progetto

Organizzativo e dei requisiti minimi di qualità degli istituti e dei servizi di cui agli articoli 256 bis e 257 bis del regolamento di esecuzione del Tulps"

- Decreto Ministero dell'interno del 04.06.2014 n° 115 "Regolamento recante disciplina delle caratteristiche e dei requisiti richiesti per l'espletamento dei compiti di certificazione indipendente della qualità e della conformità degli istituti di Vigilanza Privata autorizzati a norma art 134 Tulps"

- Disciplinare del Capo della Polizia del 24.02.2015 Allegato C

- REG 02 Regolamento Generale per l'uso del Marchio

- REG 01 Regolamento Generale per la Certificazione delle Competenze

- UNI 10459 2017 "Professionista della Security"

3. DEFINIZIONI

Per le definizioni valgono quelle riportate nella norma UNI 10459 2017 oltre che le seguenti:

Candidato: Persona che possiede i requisiti ed è stato ammesso al processo di certificazione

Commissione di esame: Organo Monocratico o Collegiale che ha le competenze per condurre un esame

Esame: Attività valutativa svolta dalla Commissione di esame

4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI PROFILI PROFESSIONALI UNI 10459 2017

Requisiti Minimi	Security Expert	Security Manager	Senior Security Manager
Grado di istruzione	Diploma di Scuola Media Superiore	Diploma di Scuola Media Superiore	Diploma di Scuola Media Superiore
Esperienza Lavorativa	(Laurea) Minimo 4 anni di esperienza professionale di Security di cui almeno 2 anni in incarichi con responsabilità e autonomia coerenti con il livello	(Laurea) Minimo 8 anni di esperienza professionale continuativa di Security di cui almeno 4 anni in incarichi con responsabilità e autonomia coerenti con il livello	(Laurea) Minimo 12 anni di esperienza professionale continuativa di Security di cui almeno 6 anni in incarichi con responsabilità e autonomia coerenti con il livello
Equipollenza	Il periodo complessivo di esperienza professionale si riduce a: 2 anni in incarichi con responsabilità e autonomia coerenti con il livello se in possesso di laurea magistrale o diploma di Master Universitario (di 1° o 2° livello) in materia di Security, 8 anni continuativi di cui almeno 4 in incarichi con responsabilità e/o autonomia coerenti con il livello se in possesso di Diploma di Scuola Media Superiore	Il periodo complessivo di esperienza professionale si riduce a: 5 anni di cui 3 in incarichi con responsabilità e autonomia coerenti con il livello se in possesso di laurea magistrale o diploma di Master Universitario (di 1° o 2° livello) in materia di Security, 12 anni continuativi di cui almeno 6 in incarichi con responsabilità e/o autonomia coerenti con il livello se in possesso di Diploma di Scuola Media Superiore	Il periodo complessivo di esperienza professionale si riduce a: 10 anni di cui 6 in incarichi con responsabilità e autonomia coerenti con il livello se in possesso di laurea magistrale o diploma di Master Universitario (di 1° o 2° livello) in materia di Security, 20 anni continuativi di cui almeno 8 in incarichi con responsabilità e/o autonomia coerenti con il livello se in possesso di Diploma di Scuola Media Superiore

Requisiti Minimi	Security Expert	Security Manager	Senior Security Manager
Formazione Specifica	Superamento di un Master di primo o secondo livello in materia di security oppure di un corso di formazione in materia di Security della durata almeno di 120 ore erogato da Università riconosciute dal Ministero dell'Istruzione, dell Università e della Ricerca oppure da Enti di formazione accreditati presso le Regioni	Superamento di un Master di primo o secondo livello in materia di security oppure di un corso di formazione in materia di Security della durata almeno di 120 ore erogato da Università riconosciute dal Ministero dell'Istruzione, dell Università e della Ricerca oppure da Enti di formazione accreditati presso le Regioni	Superamento di un Master di primo o secondo livello in materia di security oppure di un corso di formazione in materia di Security della durata almeno di 120 ore erogato da Università riconosciute dal Ministero dell'Istruzione, dell Università e della Ricerca oppure da Enti di formazione accreditati presso le Regioni
Conoscenze	Analisi Scenari e contesto, Criminologia applicata, Legislazione, Gestione del Rischio, Security Management Intelligence e security Intelligence, Strumenti di Sicurezza, Servizi di sicurezza e altri servizi, Sicurezza delle Informazioni e delle risorse intangibili, Continuità Operativa e gestione delle emergenze, Elementi di Management, Regolamento di esecuzione Tulps, D.m. 269 2010 e s.m.i. e quanto meglio previsto dal capitolo Conoscenza della Uni 10459 2017 e indicati al punto A.4	Analisi Scenari e contesto, Criminologia applicata, Legislazione, Gestione del Rischio, Security Management Intelligence e security Intelligence, Strumenti di Sicurezza, Servizi di sicurezza e altri servizi, Sicurezza delle Informazioni e delle risorse intangibili, Continuità Operativa e gestione delle emergenze, Elementi di Management, Regolamento di esecuzione Tulps, D.m. 269 2010 e s.m.i. e quanto meglio previsto dal capitolo Conoscenza della Uni 10459 2017 e indicati al punto A.4	Analisi Scenari e contesto, Criminologia applicata, Legislazione, Gestione del Rischio, Security Management Intelligence e security Intelligence, Strumenti di Sicurezza, Servizi di sicurezza e altri servizi, Sicurezza delle Informazioni e delle risorse intangibili, Continuità Operativa e gestione delle emergenze, Elementi di Management, Regolamento di esecuzione Tulps, D.m. 269 2010 e s.m.i. e quanto meglio previsto dal capitolo Conoscenza della Uni 10459 2017 e indicati al punto A.4

Requisiti Minimi	Security Expert	Security Manager	Senior Security Manager
Abilità	Abilità realizzative ed operative Abilità sociali Abilità d influenza Abilità Manageriali Abilità Cognitive Abilità di efficacia personale	Abilità realizzative ed operative Abilità sociali Abilità d influenza Abilità Manageriali Abilità Cognitive Abilità di efficacia personale	Abilità realizzative ed operative Abilità sociali Abilità d influenza Abilità Manageriali Abilità Cognitive Abilità di efficacia personale
Aggiornamento Formazione Professionale (per Mantenimento e Rinnovo Certificazione)	**Annualmente** aver partecipato ad almeno due convegni afferenti a temi di Security; oppure di aver superato un corso di aggiornamento sui temi afferenti alla Security della durata minima di 8 ore; oppure di aver svolto, in tema di Security, attività di docenza oppure pubblicato articoli o testi afferenti alla Security; Per l'ambito Disciplinare del Capo della Polizia del 24.02.2015 Attestazioni di corsi di aggiornamento, docenze, convegni, seminari, gruppo di lavoro normativo o tecnico per almeno 8 giornate complessive nei cinque anni di validità della Certificazione Assenza o corretta gestione di reclami relativi all'attività certificata Pagamento delle quote previste		

Compiti	Security Expert	Security Manager	Senior Security Manager
	Attuare le politiche, le strategie e i programmi di security definiti dal vertice aziendale/Organizzazione al fine di raggiungere gli obiettivi prefissati. Mettere in atto sistemi di controllo e di audit per verificare l'efficacia e l'efficienza dei programmi di security. Condurre le investigazioni aziendali attivate dal management o da responsabili superiori. Condurre regolari e periodiche valutazioni dei rischi e fornire assistenza ai livelli superiori per il riesame (previsto dal ciclo PDCA). Attuare programmi di informazione e di formazione in security, delle persone coinvolte nell'Organizzazione. Condurre e gestire la Security fisica (protezione delle persone, degli edifici, delle proprietà, dei beni, degli strumenti operativi dell'Organizzazione). Condurre e gestire la protezione del segreto industriale: protezione delle conoscenze, delle informazioni e dei dati appartenenti all'Organizzazione, ai propri clienti e ad altri soggetti portatori di interesse. Fornire supporto alla sicurezza delle informazioni: protezione delle conoscenze, delle informazioni appartenenti all'Organizzazione, ai propri clienti ed altri soggetti collegati portatori di interesse. Condurre e gestire il contrasto agli illeciti e alle frodi interne ed esterne: truffe e sabotaggi.	Attuare le politiche, le strategie e i programmi di security definiti dal vertice aziendale/Organizzazione al fine di raggiungere gli obiettivi prefissati. Sviluppare una struttura organizzativa per la security che descriva i compiti e i relativi responsabili. Mettere in atto sistemi di controllo e di audit per verificare l'efficacia e l'efficienza dei programmi di security. Condurre le investigazioni aziendali attivate dal management o da responsabili superiori. Condurre regolari e periodiche valutazioni dei rischi, fornire assistenza ai livelli superior per il riesame (previsto dal ciclo PDCA) ed essere inserito nel processo decisionale dell'Organizzazione per prenderne in considerazione gli aspetti critici e le loro evoluzioni. Sviluppare e attuare programmi di informazione e di formazione in security, delle persone coinvolte nell'organizzazione. Gestire la security fisica (protezione delle persone, degli edifici, delle proprietà, dei beni, degli strumenti operativi dell'Organizzazione). Gestire la protezione del segreto industriale: Protezione delle conoscenze, delle informazioni appartenenti all'Organizzazione, ai propri clienti e ad altri soggetti portatori di interesse. Gestire il supporto alla security delle tecnologie e delle strutture IT: protezione delle tecnologie,	Sviluppare una strategia di security e una politica, in linea con le strategie dell'Organizzazione, attraverso lo sviluppo e l'attuazione di un programma di security. Attuare le politiche, le strategie e i programmi di security definiti dal vertice aziendale/Organizzazione al fine di raggiungere gli obiettivi prefissati. Sviluppare una struttura organizzativa per la security che descriva i compiti e i relativi responsabili. Definire sistemi di controllo e di audit per verificare l'efficacia e l'efficienza dei programmi di security. Attivare investigazioni per verificare o per contrastare minacce interne o esterne Attivare le investigazioni aziendali richieste dal vertice dell'Organizzazione. Coordinare il processo di security, incluse la attivita di riesame (previsto dal sido PDCA) nell'Organizzazione. sviluppare programmi di informazione e di formazione in security, delle persone coinvolte Coordinare la gestione della Security fisica (protezione delle persone, degli edifici, delle proprietà, dei beni, degli strumenti operativi dell'Organizzazione). Gestire la Protezione del segreto industriale: protezione delle conoscenze, informazioni appartenenti all'Organizzazione, ai propri clienti e ad altri soggetti portatori di

	Condurre e gestire la security delle persone: protezione dell'integrità fisica dei dipendenti e dei soggetti esterni che hanno rapporti contrattuali con l'Organizzazione. Gestire incidenti ed emergenze e la continuità operativa. Condurre e gestire la security di manifestazioni/convegni tenuti dall'Organizzazione: protezione delle sedi permanenti o provvisorie in cui siano organizzati eventi d'interesse dell Organizzazione Gestire gli adempimenti di security previsti da requisiti cogenti: requisiti derivanti da leggi, regolamenti, direttive e prescrizioni obbligatorie in genere a livello locale, nazionale, europeo e internazionale. Condurre e gestire le Investigazioni e gli accadimenti afferenti alla security: attività di analisi, indagine preventiva e investigazione degli eventi dannosi interni ed esterni in collaborazione con le Autorità preposte e con i soggetti privati Porre in essere tutte le attività necessarie alla raccolta, elaborazione e gestione delle informazioni a supporto delle decisioni strategiche del business, supportando l'analisi dei contesti geopolitici: situazioni paesi, scenari per la security macroeconomici generali (Sistema economico, variabili economiche e loro interdipendenze) di settore e di mercato ("business intelligence", "competitive intelligence"). Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di conformità alle normative nazionali e internazionali ("compliance").	delle strutture informatiche dell'Organizzazione. Gestire il contrasto agli illeciti e alle frodi interne ed esterne: truffe e sabotaggi Gestire il supporto alla security delle persone: protezione dell'integrità fisica dei dipendenti e dei soggetti esterni che hanno rapporti contrattuali con l'Organizzazione. Coordinare la gestione delle emergenze, delle crisi e della continuità operativa. Coordinare Gestione security di manifestazioni/convegni dall'Organizzazione: protezione delle sedi permanenti o provvisorie in cui siano organizzati eventi d'interesse dell'Organizzazione. Coordinare gli adempimenti di security previsti da requisiti cogenti: requisiti derivanti da leggi, regolamenti, direttive e prescrizioni obbligatorie in genere a livello locale, nazionale, europeo internazionale. Coordinare le investigazioni e la gestione degli accadimenti afferenti alla security: attività di analisi, indagine preventiva e investigazione degli eventi dannosi interni ed esterni in collaborazione con le Autorità preposte e con i soggetti privati autorizzati. Porre in essere tutte le attività necessarie alla raccolta, elaborazione e gestione delle informazioni a supporto delle decisioni strategiche del business, supportando l'analisi dei contesti geopolitici: situazioni paesi, scenari per la security macroeconomici generali (sistema economico, variabili economiche e loro interdipendenze) di settore e di mercato	Coordinare il contrasto agli illeciti e alle frodi interne ed esterne: truffe e sabotaggi. Coordinare la security delle persone: protezione dell'integrità fisica dei dipendenti e dei soggetti esterni che hanno rapporti contrattuali con l'Organizzazione. Coordinare la gestione delle emergenze, delle crisi e della continuità operativa. Coordinare la gestione della security di manifestazioni/convegni dall'Organizzazione: protezione delle sedi permanenti o provvisorie in cui siano organizzati eventi d'interesse dell'Organizzazione. Coordinare gli adempimenti di security previsti da requisiti cogenti: requisiti derivanti da leggi, regolamenti, direttive e prescrizioni obbligatorie in genere a livello locale, nazionale, europeo internazionale. Coordinare le investigazioni e la gestione degli accadimenti afferenti alla security: attività di analisi, indagine preventiva e investigazione degli eventi dannosi interni ed esterni in collaborazione con le Autorità preposte e con i soggetti privati autorizzati. Coordinare tutte le attività necessarie alla raccolta, elaborazione e gestione delle informazioni a supporto delle decisioni strategiche del business, supportando l'analisi del contesti geopolitici: situazioni paesi, scenari per la security macroeconomici generali (sistema economico, variabili economiche e loro interdipendenze) di

	Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Interazione tra security e salute sul lavoro. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di interazione tra security e protezione ambientale. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Interazione tra security e responsabilità sociale. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di security e privacy. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di gestione dei rischi di origine criminosa. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Interazione con tecnologie informatiche per la gestione del "disaster recovery". Interagire con coloro che si occupano di business continuity nell'Organizzazione. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di vigilanza. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di investigazioni. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di rapporti con le autorità istituzionali, Forze dell'ordine ed Enti governativi, ecc. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano della produzione	("business intelligence", ""competitive intelligence"). Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di conformità alle normative nazionali e internazionali ("compliance"). Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di security e salute sul lavoro. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di interazione tra security e protezione ambientale. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Interazione tra security e responsabilità sociale. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di sicurezza delle informazioni e protezione dei dati personali. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di gestione dei rischi di origine criminosa. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di interazione con tecnologie informatiche per la gestione del "disaster recovery". interagire con coloro che si occupano di continuità operativa nell'Organizzazione. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di vigilanza. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Investigazioni.	settore e di mercato (business intelligence, competitive intelligence). Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di conformità alle normative nazionali e internazionali ("compliance"). Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Interazione tra security e salute sul lavoro. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di interazione tra security e protezione ambientale. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Interazione tra security e responsabilita sociale. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di security e privacy. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di gestione dei rischi di origine criminosa. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di Interazione con tecnologie informatiche per la gestione del "disaster recovery". Interazione con coloro che si occupano di "business continuity", nel caso il coordinamento della "business continuity" sia posto in altra area (per esempio "Organizzazione"). Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di vigilanza.

		Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di rapporti con le autorità istituzionali, Forze dell'ordine ed Enti governativi, ecc.. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano della produzione	Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di investigazioni. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano di rapporti con le autorità istituzionali, Forze dell'ordine ed Enti governativi, ecc.. Interagire con le strutture interne ed esterne all'Organizzazione che si occupano della produzione. Interfacciarsi con gli enti della security nazionale preposti all intelligence economica, alla sicurezza e ordine pubblico, nell'ambito della "partnership" tra pubblico e privato

5. CRITERI PER LA CERTIFICAZIONE INIZIALE

I Candidati che intendono conseguire la certificazione di competenza IBC devono far pervenire la "Domanda di Certificazione" DOC02/PG05/00 , che equivale a Contratto di Certificazione, scaricabile dal sito www.ibcert.it , alla seguente email: segreteria@ibcert.it. ,corredata dalla seguente documentazione

a) Copia del Titolo di Studio;

b) Fotografie formato tessera (in formato cartaceo o in digitale);

c) Copia di un Documento di Identità;

d) Curriculum, firmato dal Candidato, datato è redatto nei modi e nelle forme di dichiarazione sostitutiva ai sensi del DPR 445/2000;

e) Copia non autenticata del Superamento di un Master di primo o secondo livello in materia di Security oppure di un corso di formazione in materia di Security della durata almeno di 120 ore erogato da Università riconosciute dal Ministero dell'Istruzione, dell Università e della Ricerca oppure da Enti di formazione accreditati presso le Regioni. Nota: E' cura del candidato accertarsi che l'Organismo di Formazione sia in possesso dei requisiti previsti dal prospetto B1 della Uni 10459 2017.

g) Evidenza oggettiva della esperienza richiesta dallo schema di certificazione

h) Certificazione di idoneità delle caratteristiche psicoattitudinali rilasciata da uno psicologo iscritto all'ordine

Il Candidato firmando e inviando la domanda di Certificazione accetta le Condizioni Generali del Contratto, Il REG 01, il REG 02, lo schema di Certificazione e il Tariffario

5.1 ESAME DELLA DOMANDA

Al ricevimento della Domanda di Certificazione la segreteria di IBC, provvede a :

- Protocollare la domanda
- Verificare la completezza della documentazione

In caso di domanda non completa la segreteria comunica al candidato le eventuali integrazioni da produrre.

Ad esito positivo di questo riesame la segreteria invia la documentazione al Responsabile Tecnico al fine di nominare la Commissione di Esame per procedere alla analisi documentale che consiste in:

- Verifica dei Titoli in accordo a quanto richiesto dallo schema di certificazione
- Analisi degli allegati alla domanda di Certificazione

In caso di esito positivo la Commissione di Esame, per il tramite della segreteria di IBC, comunica al candidato l'esito e la prevista data di esame oltre che la prevista commissione di Esame. In caso di esito negativo la Commissione di esame, per il tramite della segreteria di IBC, comunica al candidato le motivazioni e le eventuali integrazioni da produrre.

La Domanda di Certificazione ha validità di 1 anno dalla data della sua accettazione; entro tale termine, prorogabile di ulteriori sei mesi, il processo di certificazione si deve completare. In caso contrario dovrà essere presentata una nuova Domanda di Certificazione.

5.2 ESAME PER LA CERTIFICAZIONE

L'esame di certificazione consiste in una prova scritta ed una prova orale dalla durata complessiva di quattro ore.

Prova Scritta

La prova scritta consiste in due prove. La prima prova, di carattere generale, consta di 20 domande a risposta multipla (ogni risposta esatta 1 punto); la seconda prova, consta di una trattazione di un Security Business Case (0 Non sufficiente; 60 sufficiente ; 100 esauriente). Per accedere alla prova orale i Candidati dovranno ottenere un punteggio, per ogni prova scritta, maggiore o uguale al 60 %. Il tempo concesso al candidato non è inferiore a 90 minuti e non deve superare i 120 minuti.

Prova Orale

La prova orale è volta ad accertare:

a) il possesso, da parte dei Candidati , delle caratteristiche personali previste dal singolo schema di Certificazione e della abilità alla comunicazione verbale;

b) le conoscenze e competenze generali previste dal singolo schema di certificazione;

c) le conoscenze e competenze specifiche relative agli Schemi ed ai Settori di certificazione di interesse ed alle discipline correlate.

d) approfondimento di eventuali errori effettuati nelle prove scritte

Sarà accertata anche la conoscenza sui requisiti cogenti di settore.

e) il possesso da parte dei Candidati delle competenze tecniche necessarie attraverso simulazioni di situazioni reali

g) la reale consistenza dei titoli e delle esperienze documentate dai Candidati in fase di Domanda di Certificazione.

Le domande della prova orale sono almeno quattro e afferiscono ai requisiti di conoscenza che il Professionista della Security deve possedere in accordo allo schema Uni 10459 2017 (0 non sufficiente 60 sufficiente 100 esauriente). IL tempo concesso per la prova orale è non inferiore ai 20 minuti.

Per superare la prova Orale il candidato deve ottenere una media delle valutazioni che sia uguale o maggiore al 60%

La votazione finale è costituita dalla media delle percentuali tra prove scritte e prova orale

L'esame risulta superato se la media delle prove sia uguale o maggiore al 60%

L'esito dell'esame viene comunicato all'atto della delibera della decisione della certificazione attraverso apposita comunicazione via email.

Se Il candidato supera una sola delle due prove scritte non è ammesso all orale ma la prova superata rimane valida per un anno, trascorso il quale dovrà ripetere l'esame per intero

Se il candidato ha superato le due prove scritte ma non quella orale, potrà ripetere la prova orale entro un tempo massimo di un anno. Superato tale termine il candidato dovrà ripetere l'esame per intero

Commissari di Esame: I commissari di esame sono Professionisti della Security Aziendale in possesso di Certificazione Valida in accordo alla Uni 10459. In aggiunta e per lo schema Security Manager Disciplinare Capo della Polizia i Commissari di Esame hanno competenza relativa agli istituti di Vigilanza ed i relativi servizi avendo come minimo esperienza di tre anni in Istituti di Vigilanza in ruoli di coordinamento e controllo dei servizi o due anni nelle forze dell ordine o Forze Armate in ruoli di direzione coordinamento o responsabilità di Unità Operative.

Le materie di esame sono:

Analisi Scenari e contesto; Criminologia applicata; Legislazione; Gestione del Rischio; Security Management; Intelligence e security Intelligence, Strumenti di Sicurezza; Servizi di sicurezza e altri servizi; Sicurezza delle Informazioni e delle risorse intangibili; Continuità Operativa e gestione delle emergenze; Elementi di Management; Regolamento di esecuzione Tulps; D.m. 269 2010 e s.m.i. e quanto meglio

previsto dal capitolo Conoscenza della Uni 10459 2017 e indicati al punto A.4

5.3 RILASCIO DELLA CERTIFICAZIONE DI COMPETENZA

La Commissione di esame provvede, al completamento della relativa sessione, ad inviare il Verbale di esame al RT che provvede ad individuare un Deliberatore competente per lo schema di Certificazione. Il Deliberatore provvede a riesaminare l'iter di certificazione e la completezza della documentazione registrando l'esito su apposito Form Delibera Certificazione. Completata tale fase il deliberatore invia tutta la documentazione al responsabile Tecnico che provvede ad avviare le azioni del caso al fine dell'emissione del Certificato di Competenza, con l'ausilio operativo della segreteria di IBC, indicando anche il profilo richiesto. Il Certificato, per le figure richiamate dal Disciplinare del Capo della Polizia, sarà inviato entro 60 giorni dall'emissione al Comitato Tecnico di cui all'art 260-ter comma 4 Regolamento d esecuzione TULPS, all'indirizzo dipps034.0400@pecps.interno.it

6. SORVEGLIANZA, MANTENIMENTO, RINNOVO DELLA CERTIFICAZIONE ED ESTENSIONE DELLE COMPETENZE SETTORIALI. PASSAGGIO DA ALTRO ODC

6.1 Sorveglianza e Mantenimento

Il Mantenimento della Certificazione, annuale, della Figura professionale è da ritenersi confermato a seguito di:

- Assenza di reclami da Committenti o gestione positiva di eventuali reclami ricevuti dai committenti
- Assenza di provvedimenti di IBC nei confronti della Figura professionale Certificata
- Pagamento dell'importo annuale per l'iscrizione nel registro IBC
- Quanto eventualmente previsto dal singolo Schema di Certificazione

La figura professionale certificata entro 12 mesi dal rilascio della certificazione e successivamente, ad intervalli regolari di 12 mesi è obbligato a:

- Inviare autodichiarazione di assenza di reclami o gestione positiva degli stessi
- Inviare assenza o corretta gestione di contenziosi legali in corso relativi all'attività certificata
- Pagare l'importo annuale per l'iscrizione al registro
- Fornire evidenza dell'elenco completo dei corsi di aggiornamento, partecipazione a convegni, seminari, relazioni, docenze ecc nel campo della Security aziendale
- attività specifiche svolte nel campo della security aziendale durante l'anno

I Form sono disponibili sul sito www.ibcert.it

6.2 Rinnovo

Entro 3 mesi dalla data di scadenza del Certificato (quinquennale) le figure professionali certificate e in regola con quanto previsto per il mantenimento annuale, sono tenuti a:

a) fornire auto-dichiarazione di assenza di reclami o l'evidenza della loro gestione positiva;

b) aggiornare il curriculum nelle stesse forme della prima certificazione

c) fornire la fotocopia non autenticata degli attestati di frequenza a corsi/seminari di formazione e di aggiornamento su tematiche attinenti lo schema di Certificazione frequentati negli ultimi cinque anni (la docenza di corsi/seminari viene considerata almeno equivalente alla loro frequenza) pari ad almeno 8 giornate della durata di 8 ore a giornata. (in mancanza il candidato sarà sottoposto ad esame Orale per il rinnovo)

d) fornire evidenza oggettiva dell'esperienza maturate negli ultimi cinque anni. Il rinnovo quinquennale della certificazione viene

confermato allorché si dia evidenza di avere mantenuto la competenza.

Nel Caso in cui la Figura professionale non soddisfi i requisiti, richiesti, per il rinnovo della Certificazione il RT, per il tramite della segreteria di IBC, provvede a comunicare al candidato l'esito di dover sostenere un esame orale, al cui esito positivo, sarà confermato il rinnovo della Certificazione. In caso di esito negativo il certificato sarà ritirato.

6.3 Estensione Certificazione figura professionale

Il professionista che intende fare Up Grade della Certificazione (da Security Expert a Security Manager oppure da Security Manager a Senior Security Manager) deve inoltrare richiesta a Segreteria IBC utilizzando la domanda di Certificazione presente nell'area download del sito www.ibcert.it e allegando la documentazione a sostegno della richiesta di estensione per comprovare il raggiungimento dei requisiti previsti dalla Uni 10459:2017 La Segreteria, completata la fase di riesame della completezza della domanda, provvede a inoltrare la stessa al RT affinchè proceda a nominare Commissione di esame per la verifica documentale e per la prova orale volta ad accertare il possesso delle conoscenze di quegli aspetti che differenziano lo svolgimento dei vari compiti per ogni profilo richiamato dalla Uni 10459 2017. La Commissione di esame provvede, al completamento della relativa sessione, ad inviare il Verbale di esame al RT che provvede ad individuare un Deliberatore competente per lo schema di Certificazione. Il Deliberatore provvede a riesaminare l'iter di certificazione e la completezza della documentazione registrando l'esito su apposito Form Delibera Certificazione. Completata tale fase il deliberatore invia tutta la documentazione al responsabile Tecnico che provvede ad avviare le azioni del caso al fine dell'emissione del Certificato di Competenza, con l'ausilio operativo della segreteria di IBC, indicando il profilo richiesto. In caso di esito negativo il RT, per il tramite della segreteria, provvede a comunicare al candidato la decisione.

6.4 Passaggio da altro ODC Accreditato

Il trasferimento della certificazione tra OdC accreditati, ed iscritti nell'elenco del Ministero dell'Interno per la figura Security Manager Disciplinare Capo della Polizia, di un certificato valido rilasciato ad un professionista, può essere perfezionato in qualsiasi momento, presentando richiesta IBC, redatta ai sensi della 445/2000, con allegato il certificato in corso di validità e, ove applicabile, ultima dichiarazione di mantenimento e dichiarazione del ODC cedente di assenza di pendenze tecniche ed economiche oltre che le motivazioni del passaggio. IBC provvederà ad effettuare riesame tecnico, incaricando un deliberatore qualificato, e solo al completamento con esito positivo di tale istruttoria, IBC delibererà l'emissione del proprio Certificato di Conformità, che manterrà la scadenza di quello precedente specificando che il certificato è stato emesso in precedenza da altro OdC.

IBC informerà l'OdC cedente del completamento del trasferimento entro cinque giorni dalla delibera positiva.

Qualora non siano acquisite evidenza oggettive circa l'esito dei precedenti esami (scritti e orali) il professionista che chiede il trasferimento dovrà sostenere gli esami ex novo

7 SOSPENSIONE E REVOCA DELLA CERTIFICAZIONE

L'amministratore Unico di IBC, su richiesta del RT può disporre la sospensione della Certificazione per un periodo massimo di tre mesi. Il provvedimento di sospensione è applicato nei seguenti casi:

- per sanzionare violazioni del Codice di Deontologia professionale;
- non presentazione della richiesta di rinnovo
- mancato pagamento della quota richiesta per Mantenimento o per Rinnovo Certificazione
- mancanza di integrazione della documentazione richiesta da IBC

Il provvedimento e le relative motivazioni sono trasmesse, per il tramite della segreteria, alla figura professionale certificata che ha un mese

per poter sanare le motivazioni oggetto del provvedimento di sospensione. Dal provvedimento di sospensione la figura professionale certificata ha l'obbligo di non utilizzare il Marchio IBC/Accredia e di informare i propri committenti della avvenuta sospensione.

L' amministratore Unico, su richiesta di RT, delibera la revoca della Certificazione e la cancellazione dal Registro allorché si configuri:

- mancanza di risoluzione della causa della sospensione oltre il mese concesso da IBC
- accertata violazione al Codice Etico e Deontologico
- accertata violazione allo schema di Certificazione
- Rinuncia alla Certificazione da parte del professionista

La cancellazione dal relativo registro e la revoca della Certificazione comporta per la Figura Professionale:

- non utilizzare il Marchio IBC/Accredia
- di informare i propri committenti della avvenuta cancellazione dal registro.

La Revoca e la Cancellazione dal relativo Registro sono comunicati ad Accredia per quegli schemi sotto suo Accreditamento nonché alle autorità pubbliche previste dal DM 115 2014 per la Figura Professionale Security Manager Disciplinare Capo della Polizia

8 RECLAMI E RICORSI

Si rinvia al Regolamento Generale REG 01 in versione corrente

9 USO DEL LOGO

La Figura professionale Certificata si impegna all'uso corretto del logo cosi come da REG 02 e disponibile sul sito www.ibcert.it

10. CODICE DEONTOLOGICO

La figura professionale Certificata si impegna al rispetto del Codice Deontologico declinato nel REG 01 e disponibile sul sito www.ibcert.it

4. Tabella revisioni

N° REV.	DATA	DESCRIZIONE	PARAGRAFO	PAGINA
00	06.12.21	Prima emissione	tutti	tutte
01	03.01.22	Ri-edizione integrale	tutti	tutte
02	15.01.22	Esplicitazione dei requisiti di mantenimento e rinnovo certificazione	6.1 – 6.2	11-12
03	28.04.22	Esplicitazione numerica della valutazione della prova Orale e Scritta e requisiti del Commissario di Esame – Validità delle prove	5.2	8-9
04	19.10.22	Indirizzo Email Comitato Tecnico Ministero Interno	5.3	11
05	15.03.23	Declinazione requisiti di esperienza Esaminatori Schema Disciplinare Capo della Polizia	5.2	10
06	20.06.23	Indirizzo Email Comitato Tecnico Ministero Interno	5.3	11
07	27.02.25	Esplicitazione dei termini di validità delle prove quando non superate	5.2	10
08	21.04.26	Esplicitazione dell invio, durante mantenimento certificazione, delle attività di security effettuate durante l'anno	6.1	12
09	21.05.26	Inserimento dei compiti di Security Expert, Security Manager e Senior Security Manager declinati dalla Norma Uni 10459	4	7
10	21.09.26	Aggiornamento Paragrafo 8	8	19