Icmq S.p.A. (A Socio Unico)
Società Benefit
Via G. De Castillia, 10 – 20124 Milano
Tel. 02 7015081 – Fax 02 70150854
icmq@icmq.org – www.icmq.it
P.I. 13218350158

REGOLAMENTO TECNICO
PER LA CERTIFICAZIONE DEL PERSONALE
NELL'ATTIVITA' DI

PROFESSIONISTA DELLA SECURITY

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento stabilisce i principi e i criteri per la valutazione delle competenze dei Candidati alla certificazione di "Professionista della security" e stabilisce le modalità di esecuzione e di valutazione delle prove d'esame.
Si applica indistintamente per la certificazione di:

- Professionista della security UNI 10459:2017
- Professionista della security ambito vigilanza privata UNI 10459:2017 – DM 269/2010 e s.m.i. – DM 56/2015 per le finalità previste dal Disciplinare del Capo della Polizia in data 24 febbraio 2015 – Certificazione cat. III

2. RIFERIMENTI

2.1. Riferimenti normativi di settore

- UNI 10459:2017 "Attività professionali non regolamentate – Professionista della Security - Requisiti di conoscenza, abilità e competenza"
- i documenti di cui ai riferimenti legislativi applicabili, nelle edizioni vigenti, elencati nell'Appendice F della Norma UNI 10459:2017

- DOCUMENTI AGGIUNTIVI PER L'AMBITO VIGILANZA PRIVATA:
  - DM 269/2010 "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 attuazione del TU delle leggi di pubblica sicurezza, nonché dei requisiti professionali e di capacità tecnica richiesti per la direzione dei medesimi istituti e per lo svolgimento di incarichi organizzativi nell'ambito degli stessi istituti." (di seguito DM 269/2010)
  - DM 56/2015 Regolamento recante modifiche al decreto del Ministro dell'interno 1º dicembre 2010, n. 269: «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 Testo unico delle leggi di pubblica sicurezza, nonché dei requisiti professionali e di capacità tecnica richiesti per la direzione dei medesimi istituti e per lo svolgimento di incarichi organizzativi nell'ambito degli stessi istituti.» (di seguito DM 56/2015)
  - DM 115/2014 regolamento "Disciplina delle caratteristiche e dei requisiti richiesti per l'espletamento dei compiti di certificazione indipendente dalla qualità e della conformità alle disposizioni del DM 1 dicembre 2010 e s.m.i., n.269, degli istituti di vigilanza privata, autorizzati a norma dell'art. 134 del TU delle leggi di pubblica sicurezza, e dei servizi dagli stessi offerti. Definizione delle modalità di riconoscimento degli organismi di certificazione indipendente." (di seguito DM 115/2014)
  - Disciplinare del Capo della Polizia in data 24/02/2015, per la valutazione della conformità degli istituti e dei servizi di vigilanza privata da parte degli organismi di certificazione indipendente. (di seguito Disciplinare)

2.2. Riferimenti generali

- UNI CEI EN ISO/IEC 17024 "Requisiti generali per gli organismi che operano nella certificazione del Personale".
- Legge n. 4 del 14/01/2013 "Disposizioni in materia di professioni non organizzate"
- Raccomandazione del Parlamento Europeo e del Consiglio 2009/C 155/02 del 18 giugno 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 aprile 2008, sulla costituzione del quadro europeo delle qualifiche per l'apprendimento permanente (EFQ) (Gazzetta ufficiale C 111 del 6.5.2008).
- PS DOC 01 Condizioni generali di contratto per la certificazione del personale (vedasi per tutti gli aspetti contrattuali generali)

3. SCOPO DI CERTIFICAZIONE

Il Professionista della security è la persona le cui conoscenze, abilità e competenze sono tali da garantire la gestione complessiva del processo di security o di rilevanti sotto-processi e, quando applicabile, le interazioni con altri professionisti specializzati in distinti ambiti della sicurezza (es. protezione dei dati, sicurezza delle informazioni, antifrode, tutela dei marchi e dei brevetti, salute e sicurezza sul lavoro).
Sono previsti tre livelli del profilo di Professionista della security in funzione dei contesti organizzativi di diversa complessità, costituendo un utile supporto per le organizzazioni, che possono meglio orientare le scelte sul professionista con il livello più adatto alle proprie esigenze, così come per tutte le altre parti interessate:

1. Professionista della Security di primo livello (operativo - **Security Expert**): orientato a una "media" complessità di security, considerate l'Organizzazione e le attività svolte.

   Questo profilo può avere un'esperienza di security limitata ad uno o pochi ambiti, quindi avere una visione della sicurezza settoriale (e non essere necessariamente coinvolto nella progettazione della sicurezza) ma deve essere a conoscenza dei processi e sotto-processi rilevanti, nonché attivamente coinvolto nella gestione della sicurezza.

   Profilo professionale associato al livello **EQF 5**

2. Professionista della Security di secondo livello (manageriale - **Security Manager**): orientato a una "medio-alta" complessità di security, considerate l'Organizzazione e le attività svolte.

   Questo profilo, dovrebbe avere un'esperienza di security più ampia, quindi avere una visione della sicurezza maggiormente inclusiva, non limitandosi a una conoscenza settoriale. Essendo poi un profilo manageriale deve saper gestire risorse, con un profilo uguale o inferiore al proprio, in autonomia e partecipare al processo di analisi del rischio e progettazione della sicurezza.

   Profilo professionale associato al livello **EQF 6**

3. Professionista della Security di terzo livello (alto manageriale - **Senior Security Manager**): orientato alla "massima" complessità di security, considerate l'Organizzazione e le attività svolte.

   Essendo il profilo più elevato, deve possedere un'esperienza manageriale, una visione completa e inclusiva della sicurezza, in tutti i suoi aspetti, andando oltre il concetto della semplice sicurezza fisica.
   Profilo professionale associato al livello **EQF 7**

4. RESPONSABILITA' E COMPETENZE DEL PROFESSIONISTA DELLA SECURITY

4.1. Aree di responsabilità del professionista della security

Il Professionista della security può essere coinvolto, a vario titolo, nella gestione (strategica, tattica o operativa) di ognuna delle seguenti aree di responsabilità, singolarmente, di loro combinazioni o di tutte insieme:

- Analisi di scenario e di contesto esterno;
- Analisi del contesto interno (settore, attività, processi e risorse critiche);
- Analisi dei rischi di security;
- Gestione dei rischi di security;
- Elaborazione ed attuazione piano di security;
- Elaborazione struttura organizzativa e budget di funzione;
- Attività formativa/informativa al personale dell'Organizzazione sui rischi di security;
- Antifrode;
- Antintrusione;
- Conformità alle prescrizioni legali e alle altre prescrizioni sottoscritte che riguardano la security;
- Coordinamento dei sistemi integrati di sicurezza delle strutture;

- Coordinamento della continuità operativa (Business Continuity e Disaster Recovery);
- Gestione e/o coordinamento delle risorse umane ed economiche di security;
- Gestione della vigilanza privata e dei servizi di sicurezza privati;
- Gestione delle crisi (Crisis Management);
- Gestione delle investigazioni private affidate a terzi;
- Gestione della protezione delle informazioni incluso il coordinamento e supporto alle attività relative alla sicurezza delle informazioni;
- Investigazioni;
- Business/competitive intelligence;
- Audit tecnico di security;
- Monitoraggio e "reporting" di security;
- Tutela del know-how, segreto industriale e delle risorse immateriali;
- Protezione da spionaggio industriale;
- Protezione di infrastrutture critiche;
- Protezione e tutela del management dell'Organizzazione;
- Rapporti con le Forze di polizia e Forze armate, agenzie e istituzioni pubbliche;
- Supervisione della gestione di contratti di security;
- Supporto al datore di lavoro per la tutela dei lavoratori dai rischi di origine criminosa.

4.2. Competenze del professionista della security

Ai fini del processo di certificazione di Professionista della security nei profili previsti dalla Norma UNI 10459 è richiesta l'evidenza del possesso delle competenze necessarie ai compiti attribuiti ai singoli profili.

Tale evidenza è data dalla dimostrazione di essere in grado di applicare, in relazione ai compiti del profilo, requisiti di conoscenza, abilità e capacità personali (aspetti comportamentali).

Compiti associati ai profili

- I compiti associati a ciascun profilo sono elencati nei prospetti A1, A2 e A3 della Norma UNI 10459

Conoscenze

- Le conoscenze richieste al Professionista della Security sono elencate al punto A4 A della Norma UNI 10459.

Abilità

- Le abilità richieste al Professionista della Security sono elencate al punto A5 della Norma UNI 10459.

Capacità personali (aspetti comportamentali)

- Le capacità personali richieste al Professionista della Security sono individuate nell'Appendice D della Norma UNI 10459.

5. COMPITI ASSOCIATI AI PROFILI

5.1. Compiti Livello I – Security Expert EQF 5

I compiti del profilo Livello I – Security Expert sono i seguenti:

- 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 portatori di interesse
- Condurre e gestire il contrasto agli illeciti e alle frodi interne ed esterne: truffe e sabotaggi
- 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 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 ("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 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

5.2. Compiti Livello II – Security Manager EQF 6

I compiti del profilo Livello II – Security Manager sono i seguenti:

- 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 superiori 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 e dei dati appartenenti all'Organizzazione, ai propri clienti e ad altri soggetti portatori di interesse
- Gestire la security delle informazioni: protezione delle conoscenze, delle informazioni appartenenti all'Organizzazione, ai propri clienti ed altri soggetti portatori di interesse
- Gestire il supporto alla security delle tecnologie e delle strutture IT: protezione delle tecnologie, 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 la gestione della security di manifestazioni/convegni tenuti 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 e 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 ("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
- 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

5.3. Compiti Livello III – Senior Security Manager EQF 7

I compiti del profilo Livello III – Senior Security Manager sono i seguenti:

- 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 le attività di riesame (previsto dal ciclo PDCA)

- Sviluppare programmi di informazione e di formazione in security, delle persone coinvolte nell'Organizzazione
- 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, delle informazioni appartenenti all'Organizzazione, ai propri clienti e ad altri soggetti portatori di interesse
- 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 tenuti 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 e 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 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")
- 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"
- 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 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

6. CONOSCENZE COMUNI AI PROFILI (PROFILO DI RIFERIMENTO)

Le conoscenze del profilo di riferimento sono le seguenti:

Analisi scenari e contesto

Analisi scenari di riferimento (geopolitici, sociali, economici, ambientali, tecnologici)

Analisi settore di appartenenza

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

Criminologia applicata

- Criminologia applicata e profiling criminale
- Criminalità e sicurezza nei contesti urbani (CPTED)

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 ed 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

Strumenti di sicurezza

- Tecnologie e sistemi di sicurezza passiva
- Tecnologie e sistemi di sicurezza attiva
- Strumenti organizzativi di security (policy, procedure, organizzazione, ecc…)

Servizi di sicurezza e altri servizi

- Servizi di sicurezza privata
- Vigilanza privata: servizi, contratti e normativa di riferimento
- Investigazione privata: servizi, contratti e normativa di riferimento
- Servizi ausiliari alla sicurezza (portierato, accoglienza, ecc.)

Sicurezza delle informazioni e delle risorse intangibili (intangible e information security)

- Elementi della sicurezza delle informazioni e delle risorse intangibili (marchi, know-how, …)
- Principali rischi e attacchi al sistema informatico
- Reati informatici
- Caratteristiche generali del sistema di gestione per la sicurezza delle informazioni
- Principali contromisure tecnologiche e organizzative per la sicurezza delle informazioni

Continuità operativa e gestione delle emergenze (business continuity & emergency management)

- Business Continuity e Disaster Recovery: definizione, metodologia e normativa di riferimento
- Emergency Management: definizione, metodologia, attori coinvolti, comportamento individuale e delle masse, elementi di psicologia delle emergenze, comunicazione in caso di crisi

Elementi di management

- Elementi di strategia, pianificazione e controllo aziendale
- Elementi di organizzazione del lavoro e gestione delle risorse
- Elementi di budgeting e finanza aziendale (es. strumenti di valutazione degli investimenti)
- Elementi di leadership
- Elementi di project management
- Elementi di time management
- Elementi di comunicazione e negoziazione
- Elementi di gestione dei conflitti, dello stress e del sé nei momenti critici

7. ABILITÀ COMUNI AI PROFILI (PROFILO DI RIFERIMENTO)

Abilità realizzative e operative

Orientamento al risultato

A. intensità e completezza dell'azione motivata dal risultato

B. effetto dei risultati

C. livello d'innovazione

Attenzione all'ordine, alla qualità e all'accuratezza

Spirito di iniziativa

A. orizzonte temporale

B. auto-motivazione, quantità di sforzo discrezionale

Ricerca e analisi delle informazioni

Abilità sociali

Sensibilità interpersonale

A. profondità della sensibilità interpersonale

B. capacità di ascoltare e rispondere agli altri

Orientamento al cliente

A. focalizzazione sui bisogni dei clienti

B. iniziativa (sforzo discrezionale) per aiutare o servire agli altri

Abilità d'influenza

Persuasività e influenza

A. azioni compiute per influenzare gli altri

B. portata dell'influenza, della conoscenza o della rete (interna o esterna)

Consapevolezza organizzativa

A. profondità della conoscenza dell'organizzazione

Costruzione di relazioni

A. solidità del rapporto

Abilità manageriali

Sviluppo degli altri

A. intensità dell'orientamento allo sviluppo e completezza della relativa azione

B. numero e categoria delle persone sviluppate o dirette

Attitudine al comando: assertività e uso del potere formale

A. misura dell'attitudine

Lavoro di gruppo e cooperazione

A. intensità dell'incoraggiamento del lavoro di gruppo

B. dimensione del gruppo

C. misura dello sforzo o dell'iniziativa compiuti per facilitare il lavoro di gruppo

Leadership del gruppo

A. forza del ruolo di leader

Corretta allocazione delle risorse

Abilità cognitive

Pensiero analitico

A. complessità dell'analisi

B. dimensioni dei problemi affrontati

Pensiero concettuale

A. complessità e originalità dei concetti

Abilità di efficacia personale

Autocontrollo

Fiducia in sé

A. fiducia nelle proprie possibilità

B. reazione all'insuccesso

Flessibilità

A. profondità del cambiamento

B. durata dell'azione

8. ASPETTI COMPORTAMENTALI

Il Professionista della Security adotta schemi comportamentali che richiamino e rispettino i principi integrità professionale, nel rispetto dell'operato proprio e dei colleghi/sottoposti. Nello specifico, un Professionista della Security, si assicura di agire:

- in assenza di giudizi precostituiti;
- avendo il controllo dei propri stati emotivi e operando al fine di mantenerlo o ristabilirlo in situazioni di forte stress;
- adottando strumenti che facilitino la comunicazione verbale e scritta;
- promuovendo le attività che prevedano obiettivi chiari e raggiungibili;
- mostrando interesse verso le innovazioni;
- adattandosi alle situazioni di contesto in modo tempestivo ed efficace.

9. ASPETTI PSICOATTITUDINALI

Il professionista della Security deve sottoporsi ad una valutazione delle caratteristiche psicoattitudinali, che prevede uno specifico rapporto di analisi redatto da un professionista iscritto all'ordine.

I test sono solitamente composti da 2 parti:

- metodologia quantitativa: somministrazione di un questionario sulle abilità e un questionario di personalità;
- metodologia qualitativa: un colloquio-intervista con uno psicologo del lavoro.

Il colloquio intervista completa l'indagine a cura del professionista (psicologo del lavoro).

Il colloquio intervista mira a raggiungere gli obiettivi di:

- analisi congiunta delle risultanze emerse nei questionari sull'orientamento professionale e di personalità;
- valutazione dell'adeguatezza del profilo del Candidato alla certificazione.

10. ESAME DI CERTIFICAZIONE

10.1. Requisiti di accesso all'esame

Per essere ammesso all'esame di certificazione il Candidato, in base al profilo, deve documentare i seguenti requisiti minimi:

LIVELLO I – SECURITY EXPERT	
Grado di istruzione – Apprendimento formale	Laurea di I livello (triennale).
Apprendimento non formale	Superamento di un master di 1° o 2° livello in materia di security, oppure di un corso di formazione in materia di security della durata di almeno 120 ore, erogato da Università riconosciute dal MIUR, oppure da Enti di formazione accreditati presso le Regioni[2)].
Esperienza di lavoro specifica – Apprendimento informale	Minimo 4 anni di esperienza professionale di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 2 anni in incarichi con responsabilità e autonomia coerenti con il livello. Equipollenza[1)] Se in possesso di laurea di II livello (magistrale) o di diploma di master universitario (di 1° o di 2° livello) in materia di security: il periodo complessivo di esperienza professionale si riduce a 2 anni, in incarichi con responsabilità e autonomia coerenti con il livello[3)]. Se in possesso di diploma[4)]: minimo 8 anni di esperienza professionale di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 4 anni in incarichi con responsabilità e/o autonomia coerenti con il livello.

LIVELLO II – SECURITY MANAGER	
Grado di istruzione – Apprendimento formale	Laurea di I livello (triennale).
Apprendimento non formale	Superamento di un master di 1° o 2° livello in materia di security, oppure di un corso di formazione in materia di security della durata di almeno 120 ore, erogato da Università riconosciute dal MIUR, oppure da Enti di formazione accreditati presso le Regioni[2)].
Esperienza di lavoro specifica – Apprendimento informale	Minimo 8 anni di esperienza professionale continuativa di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 4 anni in incarichi con responsabilità e autonomia coerenti con il livello[3)]. Equipollenza[1)] Se in possesso di laurea magistrale o di diploma di master universitario (di 1° o di 2° livello) in materia di security: il periodo complessivo di

	esperienza professionale continuativa si riduce a 5 anni, di cui 3 anni in incarichi con responsabilità e autonomia coerenti con il livello. Se in possesso di diploma[4)]: minimo 12 anni di esperienza professionale continuativa di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 6 anni in incarichi con responsabilità e autonomia coerenti con il livello.

LIVELLO III – SENIOR SECURITY MANAGER	
Grado di istruzione – Apprendimento formale	Laurea di I livello (triennale).
Apprendimento non formale	Superamento di un master di 1° o 2° livello in materia di security, oppure di un corso di formazione in materia di security della durata di almeno 120 ore, erogato da Università riconosciute dal MIUR, oppure da Enti di formazione accreditati presso le Regioni[2)].
Esperienza di lavoro specifica – Apprendimento informale	Minimo 12 anni di esperienza professionale continuativa di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 6 anni in incarichi con responsabilità e autonomia coerenti con il livello[3)]. Per incarichi speciali di livello manageriale, svolti come direttore della security, o membro dell'alta Direzione (top Management), in contesti internazionali ad elevata complessità, l'apprendimento non formale potrebbe coincidere con quello informale. Equipollenza[1)] Se in possesso di laurea magistrale o di diploma di master universitario (di 1° o di 2° livello) in materia di security: il periodo complessivo di esperienza professionale continuativa si riduce a 10 anni di cui 6 anni in incarichi con responsabilità e autonomia coerenti con il livello. Se in possesso di diploma[4)]: minimo 20 anni di esperienza professionale continuativa di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 8 anni in incarichi con responsabilità e autonomia coerenti con il livello.

NOTE COMUNI

Per responsabilità e autonomia si intende assumere la responsabilità di portare a termine compiti e saper adeguare il proprio comportamento alle circostanze nella soluzione dei problemi.

Per esperienza professionale continuativa si intende senza soluzione di continuità.

1) Equipollenza si intende riferita alla combinazione tra titolo di studio ed esperienza lavorativa.
2) I riferimenti giuridici, alla data di emissione della presente norma, sono (elenco esemplificativo e non esaustivo):
   - Costituzione della Repubblica Italiana – Art. 3, 4, 5, 9, 33, 34, 35, 38 e 117.
   - Legge 15 marzo 1997 n. 59 – "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la Riforma della Pubblica Amministrazione e per la semplificazione amministrativa".
   - Legge 15 maggio 1997, n. 127 – "Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo".
   - Legge 31 marzo 1998 n. 112 – "Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59".
   - DPR 8 marzo 1999 n. 275 – Regolamento recante norme in materia di autonomia delle istituzioni scolastiche, ai sensi dell'art. 21 della legge 15 marzo 1997, n. 59. (GU Serie Generale n. 186 del 10-8-1999 – Suppl. - Ordinario n. 152)
   - Legge 28 marzo 2003, n. 53 – Delega al Governo per la definizione delle norme generali sull'istruzione e dei livelli essenziali delle prestazioni in materia di istruzione e formazione professionale.
3) In questo caso, cioè l'aver frequentato e superato un Master universitario di 1° o 2° livello in materia di security, il corso di 120 ore non è necessario salvo integrazioni specifiche in base ai contenuti trattati.

4) Diploma di istruzione superiore della durata di 4 o 5 anni.

Nell'apprendimento non formale può essere considerata nel contesto dei percorsi formativi anche la valutazione delle abilità e delle caratteristiche psicoattitudinali previste dalla presente norma.
È riconosciuta la validità del percorso formativo di 90 ore, secondo la UNI 10459:1995, a condizione che venga integrato da un ulteriore percorso formativo di 30 ore, con l'ulteriore garanzia che i contenuti complessivi del corso di 90 + 30 ore siano tali da assorbire tutti i contenuti di competenze, che sono elencate nella edizione attuale della UNI 10459. Sono riconosciuti inoltre i percorsi formativi di durate superiori alle 90 ore, erogati prima del 2015 e costruiti sulla base della Norma UNI 10459:1995, purché avessero nel programma i contenuti di competenze, che sono elencate nella edizione attuale della UNI 10459. Le competenze mancanti devono essere integrate da specifici corsi.

10.2. Prima certificazione

La richiesta di certificazione deve essere formulata dal richiedente utilizzando il modulo *ps mod01 PSEC richiesta di certificazione*, indicando il profilo professionale richiesto e l'eventuale estensione all'ambito vigilanza privata.

La richiesta di certificazione dovrà essere integrata dalla documentazione prevista.

Tutti i documenti richiesti possono essere anticipati a ICMQ a mezzo posta elettronica fermo restando che i candidati dovranno recapitare a ICMQ gli originali dei documenti previsti e indicati nel modulo *ps mod01 PSEC richiesta di certificazione.*

10.3. Esaminatori ed Esperti Tecnici (Veto Power)

10.3.1. Esaminatori

Gli Esaminatori incaricati di condurre e valutare le prove d'esame, possiedono la competenza specifica nella security dimostrata con:

- esperienza lavorativa di almeno 15 anni in veste di lavoratore autonomo o dipendente, in questo ultimo caso con funzioni manageriali per almeno 10 anni;
- il soddisfacimento di tutti i requisiti previsti dall'Allegato C di cui al Disciplinare del Capo della Polizia in data 24/02/2015 (http://www.poliziadistato.it/articolo/37860).

In ogni caso costituiscono requisiti aggiuntivi:

- iscrizione in albi di consulenti tecnici istituiti presso i tribunali per le materie specifiche dell'attività/professione da certificare
- essere presenti da più di 2 anni in ruoli direttivi di associazioni professionali di categoria;
- documentata partecipazione a convegni e congressi di categoria;
- documentata attività pubblicistica nell'ambito dell'attività/professione da certificare

Gli Esaminatori, inoltre, sono a conoscenza:

- dello schema di certificazione;
- dei metodi di esame e delle registrazioni relative.

10.4. Svolgimento degli esami

Gli esami possono essere svolti sia in presenza che online (modalità da remoto) per le certificazioni dei professionisti della security aziendale.
Per i richiedenti l'estensione all'Ambito Vigilanza Privata DM 269/2010, è invece mandatorio lo svolgimento degli esami in presenza.

Struttura

Gli esami si svolgono con la presenza fisica* degli Esaminatori e consistono nell'esecuzione di:

- due prove scritte
- un colloquio individuale

**(requisito obbligatorio che si applica per il solo AMBITO VIGILANZA PRIVATA DM 269/2010).*

Le due prove scritte sono uniche per i tre livelli previsti dalla norma, ma, per quanto concerne la seconda prova scritta – caso di studio – l'approfondimento della trattazione da parte del Candidato deve essere commisurata al livello professionale oggetto della certificazione.

Prima prova scritta – set di domande: la prova ha la finalità di accertare le conoscenze richieste per il professionista della security (sia UNI 10459 che UNI 10459 con Ambito Vigilanza Privata DM 269/2010).

La prova è composta da un test scritto di **20 domande** a risposta multipla che presentano quattro risposte di cui una sola giusta e tre errate o incomplete.

Le domande a risposta multipla vengono scelte dal Responsabile Schema di Certificazione o dall'esaminatore da un elenco di domande gestite da ICMQ.

Il tempo massimo a disposizione per lo svolgimento della prova è di **30 minuti**.

Seconda prova scritta - caso di studio: la prova ha la finalità di accertare le capacità previste per le funzioni proprie del Professionista della Security (sia UNI 10459 che UNI 10459 con estensione Ambito Vigilanza Privata DM 269/2010) attraverso l'analisi e approfondimento di un tema che rappresenta una situazione reale attinente alla specifica attività professionale. Il Candidato dovrà sviluppare il tema proposto dimostrando di operare sulla base delle conoscenze e abilità necessarie per conseguire il risultato ottimale nella gestione dei rischi secondo una metodologia riferita ad un modello il più possibile aderente alla norma UNI ISO 31000.

Il caso studio viene scelto dal Responsabile Schema di Certificazione o dall'esaminatore da un elenco gestito da ICMQ, comprensivo della griglia di valutazione dei punteggi parziali. Tale griglia si compone degli elementi significativi e qualificanti del processo di gestione dei rischi che devono essere argomentati dai Candidati nelle relative esposizioni, con l'indicazione per ciascuno di essi della quota del punteggio massimo stabilito; completa la griglia una ulteriore quota di punteggio con cui tener conto anche di criteri qualificanti l'esposizione, quali ad esempio: pulizia nella composizione scritta, citazione di norme e leggi, cura nell'organizzazione del testo, ecc.. Ogni Candidato dovrà fornire una risposta appropriata e argomentare, per almeno uno dei rischi trattati, gli elementi significativi e qualificanti del processo di gestione dei rischi che caratterizzano lo sviluppo del tema.

Il tempo massimo a disposizione per lo svolgimento della prova è di **60 minuti**.

L'ammissione alla terza prova, colloquio individuale, è subordinata al superamento di entrambe le prove scritte.

Nel corso delle prove scritte lo scambio di informazioni con gli altri candidati, l'uso di cellulari, la consultazione di testi o documentazione a qualunque titolo, è causa di interruzione dell'esame e conseguente annullamento.

Prova orale - Colloquio individuale: il colloquio individuale ha la finalità di integrare e approfondire la valutazione delle capacità espresse dal Candidato durante le prove scritte e di approfondire le informazioni presentate dal Candidato.

Il colloquio riguarderà:

- approfondimenti delle conoscenze (considerando anche le risposte non complete ed esaustive delle prove scritte concluse) anche in riferimento alla proprietà dei termini utilizzati, dei concetti illustrati, delle norme applicabili e, per quanto applicabili, le norme tecniche di riferimento del settore ed inoltre, per le certificazioni nel settore della vigilanza privata, anche delle norme di riferimento che determinano il funzionamento degli istituti di vigilanza privata (DM 269/2010 e s.m.i.);
- approfondimenti circa le competenze in riferimento all'illustrazione e discussione dei processi operativi, organizzativi o gestionali relativi al livello richiesto in svariati contesti operativi e, per le certificazioni nel settore della vigilanza privata, con particolare riferimento a tale contesto;
- le esperienze professionali in riferimento ai compiti previsti per il livello richiesto e, per le certificazioni nel settore della vigilanza privata, con particolare riferimento a tale contesto;
- approccio alle prove e abilità in riferimento anche a variazioni stressogene volutamente indotte dalla commissione.

Il tempo minimo a disposizione per lo svolgimento della prova è di **20 minuti**.

Limitatamente ai Candidati alla certificazione UNI 10459 (cioè, ad esclusione di quelli con estensione all'AMBITO della VIGILANZA PRIVATA ai sensi del DM 269/2010 e s.m.i.) il colloquio individuale svilupperà maggiormente gli aspetti della conoscenza delle tematiche della security e delle esperienze professionali previsti in ambito volontario.

10.5. Valutazione delle prove d'esame

La valutazione dell'esame viene effettuata assegnando un punteggio, come descritto in dettaglio a seguire, nonché nel rispetto dei seguenti criteri:

Prima prova scritta: viene assegnato 1 punto per ogni risposta corretta (zero punti per le risposte errate o non compilate). Il punteggio minimo per superare la prova è di **12/20** (≥ 60%) corrispondenti ad almeno 12 risposte esatte.

Seconda prova scritta: viene assegnato un punteggio da zero a quaranta.

A ciascuno degli elementi significativi contenuti nella griglia di valutazione viene attribuito un punteggio parziale stabilito per la prova, in modo che il punteggio complessivo risulti pari a 40 punti. L'esposizione scritta di ciascun Candidato viene valutata attraverso un punteggio, per ognuno degli elementi definiti, compreso tra il minimo di 0 (zero) ed il valore massimo.

La prova è superata se il punteggio complessivo acquisito è di almeno:

- **24/40** (60% del punteggio massimo) per il livello I – Security Expert (EQF 5)
- **28/40** (70% del punteggio massimo) per il livello II – Security Manager (EQF 6)
- **32/40** (80% del punteggio massimo) per il livello III – Senior Security Manager (EQF 7)

Prova orale: viene assegnato un punteggio da zero a quaranta.

Durante il colloquio vengono discussi i seguenti argomenti e per ciascuno di essi, in riferimento ad altrettante specifiche griglie di valutazione, viene attribuito un punteggio variabile da 2 (valutazione minima) a 10 (valutazione massima):

- i risultati delle prove scritte;
- l'approfondimento delle conoscenze;
- le esperienze professionali;
- l'approccio alla prova.

La griglia di valutazione per la discussione delle prove scritte considera la padronanza delle materie, la prontezza e la correttezza delle risposte, la necessità di sollecitazioni dell'Esaminatore.

La griglia per l'approfondimento delle conoscenze considera il grado di competenza ed il livello di aggiornamento professionale, la necessità di sollecitazioni dell'Esaminatore.

La griglia per la valutazione delle esperienze professionali considera la maturità acquisita e in quali scenari operativi.

La griglia per la valutazione dell'approccio alla prova completa l'apprezzamento delle capacità del Candidato considerando aspetti relazionali e l'uso di linguaggio appropriato.

Il punteggio conseguito per il colloquio risulterà dalla somma delle valutazioni eseguite.

Il colloquio orale è superato se il punteggio acquisito è di almeno:

- **24/40** (60% del punteggio massimo) per il livello I – Security Expert (EQF 5)
- **28/40** (70% del punteggio massimo) per il livello II – Security Manager (EQF 6)
- **32/40** (80% del punteggio massimo) per il livello III – Senior Security Manager (EQF 7)

Nella tabella seguente è riportato nel dettaglio lo schema relativo alle valutazioni delle prove.

Tipo di prova	durata (minuti)	punteggio minimo per il superamento di ogni singola prova
Prima prova scritta set di domande	30	**12/20** (≥ 60%) per tutti i livelli
Seconda prova scritta caso di studio	60	**24/40** (≥60%) per il livello I – Security Expert **28/40** (≥70%) per il livello II – Security Manager **32/40** (≥80%) per il livello III – Senior Security Manager
Prova orale Colloquio individuale	20 minimo	**24/40** (≥60%) per il livello I – Security Expert **28/40** (≥70%) per il livello II – Security Manager **32/40** (≥80%) per il livello III – Senior Security Manager

L'esame di certificazione si considera superato se la valutazione di ogni singola prova è superiore o uguale al punteggio minimo.

10.6. Riclassificazione

Dal momento che la seconda prova estratta viene proposta identica a tutti i candidati e per tutti e tre i livelli, ciò che distingue il livello del Candidato è l'approfondimento e la maturità dello svolgimento.
A maggior ragione, il colloquio orale costituisce un momento di confronto con il Team di Esaminatori, anch'essi Professionisti della Security ed è l'unica occasione in cui si possono verificare le esperienze e le capacità del Candidato, nonché le sue abilità ed il reale livello EQF.

Limitatamente ai procedimenti di certificazione nei profili di Security Manager e Senior Security Manager, qualora la seconda prova scritta – caso di studio – o la terza prova – colloquio orale – non dovessero risultare sufficienti per il livello richiesto, in sede di esame il Team di Esaminatori può proporre al Candidato interessato la Riclassificazione del procedimento concedendo l'opportunità di conseguire la certificazione per il livello più aderente alle risultanze dell'esame.
La riclassificazione può quindi essere proposta solamente per il livello immediatamente inferiore secondo il seguente prospetto:

Livello Richiesto	Soglia superamento prove	ESITO	
Security Manager	**28/40** (≥70%)	**PUNTEGGIO 60%< x < 70%**	**PUNTEGGIO < 60%**
		Riclassificazione Security Expert	Esito negativo
Senior Security Manager	**32/40** (≥80%)	**PUNTEGGIO 70%< x < 80%**	**PUNTEGGIO < 70%**
		Riclassificazione Security Manager	Esito negativo

Il Candidato ha esplicita facoltà di accettare o rifiutare tale proposta.

Nel caso di accettazione all'ultimazione della seconda prova scritta, il Candidato sarà invitato alla prova orale che sarà condotta con riferimento ai criteri stabiliti per il livello riclassificato e, se superata, sarà proposto al Comitato Tecnico di Certificazione di ICMQ per il profilo immediatamente inferiore a quello richiesto.
Nel caso di accettazione all'ultimazione della prova orale, il Candidato sarà proposto al Comitato Tecnico di Certificazione di ICMQ per il profilo immediatamente inferiore a quello richiesto.

In caso contrario, dato atto che gli esiti delle prove sostenute e superate hanno 12 mesi di validità dalla data dell'esame, il Candidato interessato, nell'arco di tale periodo:

- potrà ripresentarsi ad una nuova sessione di esame per sostenere le prove non superate al fine di ottenere la certificazione per il livello inizialmente richiesto

ovvero

- accettare la Riclassificazione, nonché di rinunciare a ripetere la parte d'esame non sufficiente, notificando a ICMQ la sua volontà mediante comunicazione scritta.

10.7. Ripetizione dell'esame

Nel caso il Candidato venga respinto o non accetti la riclassificazione proposta dalla commissione esaminatrice, può ripetere l'esame con nuova iscrizione e versando la quota riportata nel modulo di richiesta di certificazione (PS MOD01 PSEC ripetizione di ripetizione esame), tenuto conto che le singole prove di esame superate con esito positivo, mantengono la validità per un periodo massimo di **12 mesi** dalla data dell'esame.

11. RILASCIO E DURATA DELLA CERTIFICAZIONE

Previa valutazione positiva del Comitato Tecnico di ICMQ che ratifica la certificazione, viene rilasciato il certificato di Professionista della Security nel livello conseguito e, se presente, per l'Ambito Vigilanza Privata DM 269/2010, nonché il logo ICMQ al Candidato che:

- ha soddisfatto i requisiti di ammissione all'esame
- ha superato le prove d'esame stabilite nel presente schema
- risulta in regola con tutti gli adempimenti del Regolamento Generale

La certificazione rilasciata ha una durata **quinquennale** a partire dalla data di delibera ed è soggetta a conferma di mantenimento annuale.

12. REGISTRO DELLE PERSONE CERTIFICATE

Ogni persona certificata viene iscritta nel “Registro delle persone certificate”, pubblicato sul sito www.icmq.org. Ciò consente di verificare lo stato della certificazione di Professionista della Security (validità, sospensione, revoca) nonché i dati della persona certificata.

ICMQ provvede a comunicare periodicamente ad ACCREDIA l’elenco delle persone certificate e le modifiche allo stato delle certificazioni rilasciate.

Per i certificati con estensione Ambito Vigilanza Privata DM 269/2010, ICMQ entro 60 giorni dall’emissione del certificato comunicherà al Comitato tecnico di cui all'articolo 260-ter, comma 4, del Regolamento d'esecuzione T.U.L.P.S..

13. MANTENIMENTO DELLA CERTIFICAZIONE

La validità della certificazione di ogni singola Persona certificata è subordinata alla verifica annuale (la prima entro 12 mesi dal rilascio, le altre entro successivi intervalli temporali di 12 mesi) dell’avvenuto pagamento della quota di mantenimento prevista dal Tariffario e della seguente documentazione:

- documento comprovante lo svolgimento dell’attività professionale certificata costituito dal modello ICMQ ps mod03 PSEC;
- dichiarazione resa ai sensi degli artt. 46 e 76 del DPR 445/2000 (presente e da sottoscrivere dalla Persona certificata nel modulo allegato ps mod03 PSEC) di non avere contenziosi legali in corso e/o ricevuto reclami dai propri clienti oppure, in caso di reclamo, copia della documentazione relativa alla gestione del reclamo stesso;
- dichiarazione resa ai sensi degli artt. 46 e 76 del DPR 445/2000 (presente e da sottoscrivere dalla Persona certificata nel modulo allegato ps mod03 PSEC, di assenza di condanne penali per reati non colposi anche se solo in primo grado e di provvedimenti relativi all’applicazione di misure di prevenzione, di decisioni civili e di provvedimenti amministrativi inerenti all’attività di professionista della security
- copia di eventuali documenti nei quali viene utilizzato il marchio ICMQ.

È fatta salva la facoltà di ICMQ di invitare il professionista a fornire adeguata documentazione o certificazioni a sostegno delle dichiarazioni prodotte.

In caso di carenze relative ai requisiti di mantenimento, in accordo con le condizioni generali di contratto (PS DOC 01), ICMQ provvederà a sospendere il certificato dandone comunicazione al professionista e ai registri di riferimento, secondo le tempistiche dettate dai disciplinari applicabili. La sospensione avrà una durata massima di 12 mesi, ovvero non potrà essere estesa oltre la successiva scadenza di mantenimento o rinnovo. Durante il periodo di sospensione il certificato può essere riattivato fornendo le opportune evidenze a copertura delle carenze evidenziate. In caso di mancata riattivazione, al termine del periodo di sospensione il certificato viene definitivamente revocato.

14. RINNOVO DELLA CERTIFICAZIONE

La certificazione ha una durata di cinque anni e può essere rinnovata previa esecuzione della verifica dell’avvenuto pagamento degli importi previsti dal Tariffario per il rinnovo e dell’acquisizione documentata di almeno 40 crediti formativi complessivi, cioè di 8 crediti formativi annui, dell’impegno complessivo di almeno 8 giornate nei 5 anni di validità della certificazione (vedi NOTA).

In caso di mancata acquisizione dei crediti formativi richiesti nell’ultimo anno di mantenimento e dell’evidenza del richiamato impegno di 8 giornate, il rinnovo della certificazione è subordinato ad un colloquio orale *(con un Esaminatore obbligatoriamente in presenza fisica per il solo AMBITO VIGILANZA PRIVATA DM 269/2010)* analogo a quello di prima certificazione aggiuntivo alla verifica documentale, da sostenere prima della scadenza del certificato (dopo tale scadenza il certificato non potrà più ritenersi valido e, pertanto, non potrà essere rinnovato).

NOTA:

L'impegno di ogni Persona certificata per il suo aggiornamento professionale è richiesto per le discipline, tematiche ed argomenti riconducibili esclusivamente alla security e alla sua evoluzione di contesto; tale impegno viene valutato in crediti formativi con i seguenti criteri:

▪ partecipazione a convegni/seminari e/o corsi di formazione afferenti a temi di Security privi di verifica finale	0,5 crediti all'ora
▪ partecipazione a corsi di formazione/aggiornamento afferenti a temi di Security con superamento della verifica finale	1 credito ogni ora
▪ pubblicazione di testi in tema di Security con case editrici di livello nazionale	1 testo = 8 crediti
▪ pubblicazione di articoli in tema di Security su riviste specializzate	1 articolo = 1 credito
▪ attività di docenza in materie di Security	1 ora di docenza = 1 credito

Si specifica che il raggiungimento dei 40 crediti formativi prima della scadenza quinquennale non esenta dal dover proseguire nella formazione continua, ovvero dall'acquisizione degli 8 crediti formativi per ogni anno rimanente al rinnovo.

Ricevuta la suddetta documentazione, ICMQ esamina la conformità dei requisiti per la correttezza del rinnovo in relazione ai regolamenti di riferimento e, ad esito positivo, delibera il rinnovo per ulteriori 5 anni.

15. PASSAGGIO DI LIVELLO

Il Professionista, certificato ICMQ sulla base del presente schema, può richiedere di sostenere l'esame di passaggio al successivo livello (per il medesimo ambito di certificazione) al raggiungimento dei requisiti di ammissione per esso previsti.

La richiesta di passaggio di livello può essere avanzata:

- contestualmente al mantenimento/rinnovo della sua certificazione in essere;
- su specifica richiesta durante il periodo di validità della certificazione posseduta.

La richiesta di passaggio richiede l'integrazione della documentazione prodotta per la prima certificazione, sulla base di quanto richiesto dal modulo PS MOD01 PSEC, ed il pagamento della quota prevista a tal fine nel tariffario in vigore.

ICMQ provvede a:

- esaminare la documentazione prodotta dal professionista certificato per accertare il possesso dei requisiti per il livello richiesto;
- (eventualmente) richiedere informazioni/documenti supplementari;

Qualora venissero riscontrate carenze per il passaggio richiesto, l'iter di valutazione viene interrotto e il Professionista informato della necessità di rimuovere le carenze riscontrate.

Nel caso di riscontro positivo, ICMQ provvede a:

- invitare il Professionista ad una sessione d'esame per sostenere un colloquio di approfondimento (vedi paragrafo 15.1 e NOTA)
- sottoporre l'esito delle suindicate attività alla struttura di ICMQ cui compete l'approvazione della proposta di passaggio di livello, la quale nel caso di superamento dell'esame:
- rilascia la nuova certificazione chiedendo la restituzione/ distruzione di quello superato;
- aggiorna il registro applicabile dei Professionista della Security certificati
- effettua le comunicazioni obbligatorie (si veda paragrafo 12).

Il cambio di livello non comporta la variazione della data di scadenza del certificato.

NOTA: il colloquio di approfondimento si svolge con la presenza fisica degli Esaminatori per il solo Ambito Vigilanza Privata DM 269/2010, mentre può essere svolto anche da remoto in assenza di tale estensione.

15.1. Esami per il passaggio di livello

Il colloquio con l'esaminatore qualificato riguarderà l'analisi e la discussione di uno o più esempi di situazioni operative di complessità appropriata al livello richiesto, e per le certificazioni nel settore della vigilanza privata con particolare riferimento a tale contesto, e valuterà:

- le conoscenze in riferimento alla proprietà dei termini utilizzati e concetti illustrati;
- le competenze in riferimento all'illustrazione dei processi operativi, organizzativi e gestionali relativi al livello richiesto;
- le esperienze professionali in riferimento ai compiti previsti per il livello richiesto;
- approccio alla prova e abilità in riferimento anche a variazioni stressogene volutamente indotte dalla commissione.

Al colloquio individuale viene assegnato un punteggio **da zero a quaranta**.
Durante il colloquio verranno discussi gli argomenti sopraindicati e per ciascuno di essi, in riferimento ad altrettante specifiche griglie di valutazione, viene attribuito un punteggio variabile da 2 (valutazione minima) a 10 (valutazione massima).

Il punteggio conseguito per il colloquio risulterà dalla somma delle valutazioni eseguite. Il colloquio orale è superato se il punteggio acquisito è di almeno **28/40** (70% del punteggio massimo) nel caso di passaggio da I livello Security Expert a II livello Security Manager, o **32/40** (80% del punteggio massimo) nel caso di passaggio da II livello Security Manager a III livello Senior Security Manager.

16. ESTENSIONE

Il Professionista certificato ICMQ sulla base del presente schema in qualità di Professionista della Security in uno dei livelli previsti dalla norma UNI 10459:2017, può richiedere il rilascio del certificato in ambito Vigilanza Privata in conformità ai requisiti applicabili del DM 269/2010 e s.m.i., al DM 115/2014 e al Disciplinare del Capo della Polizia del 24.02.205:

- contestualmente al mantenimento/rinnovo/passaggio di livello della certificazione in essere
- su specifica richiesta durante il periodo di validità della certificazione posseduta.

La richiesta di estensione (ed eventuale passaggio di livello) richiede l'integrazione della documentazione prodotta per la prima certificazione, sulla base di quanto richiesto dal modulo PS MOD 01 PSEC ed il pagamento della quota prevista a tal fine nel tariffario in vigore.

ICMQ provvede a:

- esaminare la documentazione prodotta dal professionista certificato;
- (eventualmente) richiedere informazioni/documenti supplementari da sottoporre alla valutazione della Commissione Deliberante secondo Tariffario[4].

Nel caso di riscontro positivo, ICMQ, provvede a:

- invitare il Professionista ad una sessione d'esame per sostenere un colloquio di approfondimento che riguarderà conoscenze, competenze ed esperienze professionali relativi all'Ambito Vigilanza Privata DM 269/2010.
- sottoporre l'esito delle suindicate attività alla struttura di ICMQ cui compete l'approvazione della proposta di estensione, la quale nel caso di superamento dell'esame:
- rilascia la nuova certificazione chiedendo la restituzione/ distruzione di quello superato;
- aggiorna il registro applicabile dei Professionista della Security certificati;
- effettua le comunicazioni obbligatorie (si veda paragrafo 12), in particolare, in conformità alle prescrizioni del Disciplinare del Capo della Polizia in data 24.02.2015.

[4] esempio verifica documentazione relativa alla formazione specifica (apprendimento non formale) acquisita frequentando e superando corsi non qualificati da ICMQ

Qualora l'estensione avvenga in concomitanza del rinnovo della precedente certificazione, sarà emesso un nuovo certificato con scadenza quinquennale.

16.1. Esami di estensione

Il colloquio di approfondimento riguarda l'analisi e la discussione di uno o più esempi di situazioni operative proprie dell'Ambito Vigilanza Privata DM 269/2010.

Il colloquio è finalizzato a valutare:

- le conoscenze in riferimento alla proprietà dei termini utilizzati e concetti illustrati oltre che del complesso normativo di riferimento che determinano il funzionamento degli istituti di vigilanza privata (DM 269/2010 e s.m.i.) e, per quanto applicabili, le norme tecniche di riferimento del settore;
- le competenze in riferimento all'illustrazione dei processi operativi, organizzativi e gestionali proposti nel contesto della vigilanza privata;
- le esperienze professionali in riferimento e in particolare nel contesto della vigilanza privata;
- approccio alla prova e abilità in riferimento anche a variazioni stressogene volutamente indotte dalla commissione.

Al colloquio individuale viene assegnato un punteggio da **zero** a **quaranta**.

Durante il colloquio verranno discussi gli argomenti sopraindicati e per ciascuno di essi, in riferimento ad altrettante specifiche griglie di valutazione, viene attribuito un punteggio variabile da 2 (valutazione minima) a 10 (valutazione massima).

Il punteggio conseguito per il colloquio risulterà dalla somma delle valutazioni eseguite. Il colloquio orale è superato se il punteggio acquisito è di almeno:

- **24/40** (60% del punteggio massimo) per l'estensione di un certificato di I livello Security Expert;
- **28/40** (70% del punteggio massimo) per l'estensione di un certificato di II livello Security Manager;
- **32/40** (80% del punteggio massimo) per l'estensione di un certificato di III livello Senior Security Manager.

Nel caso di contestuale passaggio di livello il punteggio dovrà essere coerente con il livello richiesto (si veda paragrafo 15.1).

16.2. Riduzione

Il professionista certificato con estensione all'Ambito Vigilanza Privata DM269, può richiedere in fase di mantenimento o rinnovo, la riduzione della propria certificazione all'ambito Aziendale presentando apposita domanda tramite il modulo ps mod01 PSEC_riduzione.
ICMQ provvederà a riemettere il certificato aggiornato mantenendone invariate le date di prima emissione e di scadenza, nonché ad aggiornare i registri ICMQ ed Accredia, informando al contempo il Ministero della riduzione effettuata revocando di fatto il precedente certificato DM 269.

17. TRASFERIMENTO

Il Professionista della Security certificato:

- da altro OdC accreditato per la Norma UNI 10459:2017;
- da altro Organismo di Certificazione Indipendente (riconosciuto dal Ministero dell'Interno) nel settore della Vigilanza Privata

può richiedere a ICMQ il trasferimento della sua certificazione valida – solo per lo stesso ambito e per lo stesso livello – compilando al riguardo il modulo ps mod01 PSEC_TR.

NOTA BENE:
Non sono accettabili le richieste di passaggio di livello e/o di estensione contestuali al trasferimento sopra descritto della certificazione.
Tali richieste possono essere valutate ed eventualmente effettuate solo una volta deciso il trasferimento, rilasciata la nuova certificazione ed aggiornato il registro (e con le comunicazioni obbligatorie avvenute per l'Ambito Vigilanza).

17.1. Trasferimento UNI 10459

ICMQ accoglie la domanda di trasferimento solo se accompagnata da:

- la copia del certificato in essere in corso di validità;
- una sintesi degli esiti relativi al precedente esame;
- l'evidenza di chiusura di eventuali pendenze (economiche e tecniche) nei confronti dell'OdC cedente, compresa la gestione di eventuali reclami;
- il pagamento della quota prevista nel tariffario in vigore.

ICMQ provvede a:

- esaminare la documentazione prodotta dal professionista certificato;
- (eventualmente) richiedere informazioni/documenti supplementari.

Qualora venissero riscontrate carenze per il trasferimento richiesto, l'iter di valutazione viene interrotto e il Professionista informato della necessità di rimuovere le carenze riscontrate.

Nel caso di riscontro positivo, **tenendo conto del medesimo ambito e livello certificato oggetto della richiesta di trasferimento**, ICMQ provvede a:

- sottoporre l'esito delle suindicate attività alla Commissione Deliberante di ICMQ cui compete la decisione di trasferimento;
- rilasciare in seguito la nuova certificazione;
- aggiornare il registro dei Professionisti della Security certificati.

17.2. Trasferimento UNI 10459 Ambito Vigilanza Privata DM269

ICMQ accoglie la domanda di trasferimento solo se accompagnata da:

- la copia del certificato in essere in corso di validità;
- una sintesi degli esiti relativi al precedente esame (prova teorica e prova pratica);
- l'evidenza di chiusura di eventuali pendenze (economiche e tecniche) nei confronti dell'OdCI cedente, compresa la gestione di eventuali reclami;
- il pagamento della quota prevista nel tariffario in vigore
- una dichiarazione ai sensi del DPR 445/2000 (art 47 e 76) in ordine a:
  - reclami o contenziosi relativi alle attività effettuate nello schema specifico;
  - numero e la tipologia degli interventi effettuati dalla data dell'ultimo rinnovo della certificazione con i relativi riferimenti;
  - motivazioni per la richiesta di trasferimento.

ICMQ provvede a:

- esaminare la documentazione prodotta dal professionista certificato;
- (eventualmente) richiedere informazioni/documenti supplementari.

Qualora venissero riscontrate carenze per il trasferimento richiesto, l'iter di valutazione viene interrotto e il Professionista informato della necessità di rimuovere le carenze riscontrate.

Nel caso di riscontro positivo, **tenendo conto del medesimo ambito e livello certificato oggetto della richiesta di trasferimento**, ICMQ provvede a:

- sottoporre l'esito delle suindicate attività alla Comitato Tecnico di ICMQ cui compete la decisione di trasferimento;
- rilasciare in seguito la nuova certificazione;
- aggiornare il registro dei Professionisti della Security certificati;
- effettuare le comunicazioni obbligatorie previste dal Disciplinare del Capo della Polizia del 24.02.2015.