STATO DELLE REVISIONI		
rev. n°	SINTESI DELLA MODIFICA	DATA
5	Adeguamento all'edizione 2017 della Norma UNI 11506	2018-04-10
4	Aggiornamento documento e Rebranding	2017-07-21

VERIFICA	Direttore Qualità & Industrializzazione Maria Anzilotta *Firma su cartaceo*
APPROVAZIONE	Chief Operating Officer Giampiero Belcredi *Firma su cartaceo*

SOMMARIO

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento contiene i requisiti specifici per la certificazione dell'"Informatico Professionista" relativamente allo specifico profilo di **ICT Security Manager.**

In particolare il presente documento denominato **Scheda del Profilo Professionale** definisce univocamente:

- Descrizione del profilo professionale
- Elenco delle evidenze che il candidato deve produrre a soddisfazione dei requisiti
- Requisiti di Istruzione, Conoscenza, Competenza ed esperienza professionale
- Requisiti per l'accesso all'esame di certificazione
- Modalità per lo svolgimento dell'esame di certificazione (composizione della commissione, criteri di valutazione, tipo, durata e svolgimento delle prove)
- Requisiti e modalità per il mantenimento della certificazione
- Requisiti e modalità per il rinnovo della certificazione.

Tutte le regole generali riferite alla certificazione dell'Informatico Professionista sono riportate nella Procedura di schema PG_PRS_ICT_Professional_BASE a cui tale scheda è abbinata e a cui si rimanda.

2 SCHEDA PROFILO PROFESSIONALE

Il presente documento è redatto in conformità alla norma ISO 17024:2012 per professionisti che svolgono l'attività di:

ICT-Security Manager (UNI 11621-2 – profilo n°11)

In conformità alla norma UNI 11506:2017 e ai regolamenti europei ai quali essa si ispira e a cui rimanda.

2.1 Terminologia

I livelli indicati per la definizione delle e-competence sono stabiliti nel quadro

livello e-CF	livello EQF	cicli EU	livello istruzione
e-5	**8**	**III ciclo**	dottorato PHD (higher Education)
e-4	**7**		Laurea Magistrale/Master Universitario (higher Education)
e-3	**6**		Laurea/Bachelor (higher Education)
e-2	**5**	**II ciclo**	Istruzione Tecnica Superiore (Further Education)
	4		Istruzione Secondaria (Secondary School)
e-1	**3**	**I ciclo**	Istruzione Secondaria Primo Grado (Italy)

- **Accountable – Garantisce**

Essere Accountable vuol dire essere l'unico "owner" del lavoro. L'owner deve terminare o approvare un task, un obiettivo o una decisione quando questi sono completati. L'owner si deve assicurare che le responsabilità siano assegnate per tutte le attività collegate. C'è solo un owner accountable per ciascun deliverable. Il termine "accountability" è anche usato come termine generico , senza che ci sia una relazione con la matrice RACI.

- **Responsible – Assicura**

Le "Persone che fanno" un lavoro sono responsabili per quel lavoro. Essi devono realizzare il task o l'obiettivo o prendere le relative decisioni. Più persone possono essere insieme responsabili di un

deliverable. I termini " responsabile" e "responsibilità" sono anche usati come termini generici, senza relazione con la Matrice RACI.

- **Contributor – Contribuisce**

I contributori forniscono contributi prima che il lavoro sia completato o terminato. Sono partecipanti attivi e "in the loop". Più persone possono essere contributori di un deliverable.

2.2 Descrizione sintetica del profilo

Estratto dal Documento CWA 16458 - European ICT Professional Profiles.

Titolo del Profilo	**ICT SECURITY MANAGER (11) (MANAGER DELLA SICUREZZA ICT)**		
Descrizione sintetica	Gestisce la politica di sicurezza del Sistema di Informazioni.		
Missione	Definisce la politica di sicurezza del Sistema di Informazioni. Gestisce la diffusione delle sicurezza attraverso tutti i sistemi informativi. Assicura la fruizione delle informazioni disponibili. Riconosciuto come l'esperto di politica di sicurezza ICT dagli stakeholder interni ed esterni.		
Deliverable	**Accountable**	**Responsible**	**Contributor**
	• Politica Sicurezza Informazioni	• Base di conoscenza o informazione • Strategia Sicurezza Informazioni	• Politica di gestione dei rischi • Proposta integrazione nuove tecnologie • Strategia SI e sua implementazione
Task principali	• Definisce ed implementa procedure connesse con la sicurezza del SI • Contribuisce allo sviluppo della politica di sicurezza dell'organizzazione • Mette a punto il piano di prevenzione • Informa e incrementa la consapevolezza del management aziendale • Assicura la promozione delle norme di sicurezza IT tra gli utenti • Controlla ed assicura che i principi e le regole per la sicurezza del SI siano applicati		
e-competence *(da e-CF)*	A.7. Osservatorio Tecnologico		Livello 4
	D.1. Sviluppo della Strategia della Sicurezza Informatica		Livello 5
	E.3. Gestione del Rischio		Livello 3
	E.9. IT Governance		Livello 4
	E.8. Gestione della Sicurezza dell'Informazione		Livello 4
Area di applicazione dei KPI	Efficacia delle Policy di Sicurezza		

2.2.1 Dettaglio e-competenze secondo CWA 16234 parte I

ICT SECURITY MANAGER (MANAGER DELLA SICUREZZA ICT)		
Dimensione 2 – e-competence **Dimensione 3 – livelli di capacità**	**Dimensione 4 – knowledge** ***Conosce/ E' informato su/ Ha familiarità con;***	**Dimensione 4 – skill** ***E' capace di;***
A. PLAN (PIANIFICARE)		
A.7. Osservatorio Tecnologico (Technology Watching) Esplora gli ultimi sviluppi tecnologici dell'ICT per comprenderne l'evoluzione tecnologica. Concepisce soluzioni innovative per l'integrazione di nuove tecnologie nei prodotti, applicazioni e servizi esistenti o per la creazione di nuove soluzioni.	• K1 le tecnologie emergenti e le applicazioni più importanti del mercato • K2 le necessità del mercato • K3 le sorgenti d'informazione più importanti (e.g. riviste, conferenze e eventi, newsletter, opinion leader, etc.) • K4 le regole di discussione nelle comunità web	• S1 monitorare le sorgenti di informazione e seguire le più promettenti con continuità • S2 identificare venditori e fornitori delle soluzioni più promettenti; valutare, giustificare e proporre i più appropriati. • S3 identificare i vantaggi e i miglioramenti del business derivanti dall'adozione delle tecnologie emergenti • S4 verificare la soluzione progettata (proof of concept)
Livello 4 – Impiega un ampio spettro di conoscenze specialistiche di tecnologie nuove ed emergenti, accoppiata ad una profonda conoscenza del business, per immaginare e articolare le soluzioni del futuro.Fornisce una guida esperta e consiglia, i gruppi della dirigenza nel business e nella tecnologia circa le potenziali innovazioni a supporto delle decisioni strategiche		
Livello 5 – Esercita la leadership strategica. Immagina e articola le soluzioni future e dirige l'organizzazione nel costruirle e nell'impiegarle.		
D.ENABLE (ABILITARE)		
D.1. Sviluppo della Strategia della Sicurezza Informatica (Information Security Strategy Development) Definisce e rende applicabile formalmente la strategia, gli obiettivi e la cultura organizzativa al fine di mantenere la sicurezza e la difesa dei dati. Fornisce la base per la gestione della Sicurezza dell'informazione, compresa l'identificazione dei ruoli e delle responsabilità (ref D.2). Usa gli standard definiti per determinare gli obiettivi per l'integrità, la disponibilità e la privacy delle informazioni.	• K1 il potenziale e le opportunità offerte dagli standard e dalle best practice più rilevanti. • K2 l'impatto dei requisiti legali sulla sicurezza dell'informazione • K3 la strategia dell'informazione nell'organizzazione • K4 le possibili minacce alla sicurezza	• S1 sviluppare ed analizzare criticamente la strategia aziendale sull'information security • S2 definire, presentare e promuovere una politica dell'sicurezza dell'informazione presso il senior management dell'organizzazione • S3 applicare gli standard,le best practice e i requisiti legali più rilevanti alla sicurezza dell'informazione • S4 anticipare i cambiamenti richiesti alla strategia aziendale della sicurezza dell'informazione e formulare nuovi piani • S5 proporre misure efficaci di contingenza
Livello 4 – Impiega l'esperienza		

ICT SECURITY MANAGER (MANAGER DELLA SICUREZZA ICT)		
Dimensione 2 – e-competence **Dimensione 3 – livelli di capacità**	**Dimensione 4 – knowledge** ***Conosce/ E' informato su/ Ha familiarità con;***	**Dimensione 4 – skill** ***E' capace di;***
approfondita e fa leva su standard esterni e best practice.		
Livello 5 – Esercita la leadership strategica per radicare la Sicurezza dell'informazione nella cultura dell'organizzazione.		
E.MANAGE (GESTIRE)		
E.3. Gestione del Rischio (Risk Management) Implementa la gestione del rischio dei sistemi informativi attraverso l'applicazione delle politiche e procedure definite dall'azienda per la gestione del rischio. Valuta il rischio per il business dell'organizzazione e documenta rischi potenziali e piani di prevenzione.	• K1 i valori ed interessi dell'azienda cui applicare l'analisi del rischio • K2 il ritorno dell'investimento comparato all'annullamento del rischio • K3 le buone pratiche (metodologie) e gli standard nella analisi del rischio	• S1 sviluppare piani di gestione del rischio per identificare le necessarie azioni preventive • S2 comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio • S3 progettare e documentare I processi dell'analisi e della gestione del rischio • S4 applicare azioni di contenimento del rischio e di emergenza
Livello 2 – Comprende ed applica principi della gestione del rischio e ricerca soluzioni ICT per mitigare I rischi identificati		
Livello 3 – Decide sulle azioni più appropriate per adeguare la sicurezza e affrontare l'esposizione al rischio. Valuta, gestisce le eccezioni e ne assicura la validazione; conduce visite ispettive sui processi ICT e sull'ambiente.		
Livello 4 – Fornisce leadership per definire e rendere applicabile una politica di gestione del rischio considerando tutti i possibili vincoli, inclusi gli aspetti tecnici, economici e politici. Delega incarichi		
E.MANAGE (GESTIRE)		
E.8. Gestione della Sicurezza dell'Informazione (Information Security Management) Implementa la politica della sicurezza dell'informazione. Controlla e prende iniziative a fronte di intrusioni, frodi e buchi o falle della sicurezza. Assicura che i rischi legati alla sicurezza siano analizzati e gestiti per i dati e le informazioni aziendali. Rivede gli incidenti sulla sicurezza e fornisce raccomandazioni per un miglioramento continuo della sicurezza.	• K1 la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti • K2 le best practice e gli standard nella gestione della sicurezza delle informazioni • K3 I rischi critici per la gestione della sicurezza • K4 l'approccio all'attività ispettiva interna del sistema informativo	• S1 documentare la politica di gestione della sicurezza collegandola alla strategia di business • S2 analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi • S3 costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi • S4 effettuare l'attività ispettiva di sicurezza
Livello 2 – Controlla sistematicamente l'ambiente per identificare e definire minacce e debolezze. Registra e denuncia le mancanze.		

ICT SECURITY MANAGER (MANAGER DELLA SICUREZZA ICT)		
Dimensione 2 – e-competence **Dimensione 3 – livelli di capacità**	**Dimensione 4 – knowledge** ***Conosce/ E' informato su/ Ha familiarità con;***	**Dimensione 4 – skill** ***E' capace di;***
Livello 3 – Valuta le misure e gli indicatori di gestione della sicurezza e decide della loro compatibilità con la politica della sicurezza delle informazioni. Indaga ed adotta misure correttive per affrontare eventuali violazioni della sicurezza		
Livello 4 – Fornisce la leadership per l'integrità, la riservatezza e la disponibilità dei dati presenti nei sistemi informativi e ed assicura la conformità con i requisiti legali		
E.MANAGE (GESTIRE)		
E.9. IT Governance (IT Governance) Definisce, realizza e controlla la gestione dei sistemi informativi in linea con i vincoli di business. Tiene conto di tutti i parametri interni ed esterni come la normativa e l'aderenza agli standard industriali per indirizzare la gestione del rischio e dell'impiego delle risorse al fine di raggiungere i benefici di business messi a bilancio.	• K1 l'infrastruttura ICT e l'organizzazione del mercato • K2 la strategia di mercato dell'azienda • K3 I valori del mercato K4 I requisiti legali	• S1 gestire modelli di governance applicabili • S2 analizzare il contesto di business dell'azienda e la sua evoluzione • S3 definire ed implementare adeguati indicatori di prestazione (KPI's) • S4 comunicare il valore, I rischi e le opportunità derivanti dalla strategia del sistema informativo
Livello 4 – Fornisce la leadership per la governance della strategia dell'IT comunicando, diffondendo e controllando i principali processi in tutta la infrastruttura IT.		
Livello 5 – Definisce ed adegua la strategia di governance dell'IT inserendola all'interno della strategia complessiva dell'organizzazione aziendale. Adatta la strategia di governance IT per prendere in considerazione nuovi, significativi eventi derivanti da aspetti legali, economici, politici, di mercato o ambientali.		

2.3 Requisiti

2.3.1 Idoneità

Non ci sono elementi specifici che determinano l'idoneità dei candidati

2.3.2 Affidabilità giuridica

Per poter accedere al processo di certificazione il candidato dovrà sottoscrivere una dichiarazione ai sensi del DPR 445 sulla propria affidabilità giuridica e onorabilità professionale.

2.3.3 Istruzione

Laurea magistrale + Dottorato

in alternativa alla Laurea e Dottorato: 10 anni di esperienza nella sicurezza informatica

*Tabella di normalizzazione delle e-competence in termini di **istruzione***

livello e-CF	*livello EQF*	*cicli EU*	*livello istruzione*	*Equipollenza (educazione informale)*
e-5	***8***	***III ciclo***	*dottorato PHD (higher Education)*	*10 anni esperienza*
e-4	***7***		*Laurea Magistrale/Master Universitario (higher Education)*	*7 anni esperienza*
e-3	***6***		*Laurea/Bachelor (higher Education)*	*5 anni esperienza*
e-2	***5***	***II ciclo***	*Istruzione Tecnica Superiore (Further Education)*	*2 anni esperienza*
	4		*Istruzione Secondaria (Secondary School)*	
e-1	***3***	***I ciclo***	*Istruzione Secondaria Primo Grado (Italy)*	*1 anno esperienza*

2.3.4 Conoscenze di Base, Trasversali e Tecnico Professionali

- Tutte le prove d'esame sono svolte in Italiano e il candidato deve dimostrare di poter comprendere testi scritti e di saper condurre una conversazione tecnica professionale.
- Conoscenza della lingua inglese tale da permettere la comprensione di testi tecnici articolati e complessi inerenti allo specifico settore professionale (requisito dichiarato attraverso l'autocertificazione nella domanda di certificazione e verificato in sede d'esame nella seconda prova scritta.)

Conosce/ E' informato su/ Ha familiarità con;
• le tecnologie emergenti e le applicazioni più importanti del mercato • le necessità del mercato • le sorgenti d'informazione più importanti (e.g. riviste, conferenze e eventi, newsletter, opinion leader, etc.) • le regole di discussione nelle comunità web
• il potenziale e le opportunità offerte dagli standard e dalle best practice più rilevanti. • l'impatto dei requisiti legali sulla sicurezza dell'informazione • la strategia dell'informazione nell'organizzazione • le possibili minacce alla sicurezza
• i valori ed interessi dell'azienda cui applicare l'analisi del rischio • il ritorno dell'investimento comparato all'annullamento del rischio • le buone pratiche (metodologie) e gli standard nella analisi del rischio
• la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti • le best practice e gli standard nella gestione della sicurezza delle informazioni • I rischi critici per la gestione della sicurezza • l'approccio all'attività ispettiva interna del sistema informativo
• l'infrastruttura ICT e l'organizzazione del mercato • la strategia di mercato dell'azienda • I valori del mercato • I requisiti legali

2.3.5 Competenze Tecnico-Professionali specialistiche

E' capace di;
• monitorare le sorgenti di informazione e seguire le più promettenti con continuità • identificare venditori e fornitori delle soluzioni più promettenti; valutare, giustificare e proporre i più appropriati. • identificare i vantaggi e i miglioramenti del business derivanti dall'adozione delle tecnologie emergenti • verificare la soluzione progettata (proof of concept)
• sviluppare ed analizzare criticamente la strategia aziendale sull'information security • definire, presentare e promuovere una politica dell'sicurezza dell'informazione presso il senior management dell'organizzazione • applicare gli standard,le best practice e i requisiti legali più rilevanti alla sicurezza dell'informazione • anticipare i cambiamenti richiesti alla strategia aziendale della sicurezza dell'informazione e formulare nuovi piani • S5 proporre misure efficaci di contingenza
• sviluppare piani di gestione del rischio per identificare le necessarie azioni preventive • comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio • progettare e documentare I processi dell'analisi e della gestione del rischio • applicare azioni di contenimento del rischio e di emergenza
• documentare la politica di gestione della sicurezza collegandola alla strategia di business • analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi • costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi • effettuare l'attività ispettiva di sicurezza
• gestire modelli di governance applicabili • analizzare il contesto di business dell'azienda e la sua evoluzione • definire ed implementare adeguati indicatori di prestazione (KPI's) • comunicare il valore, I rischi e le opportunità derivanti dalla strategia del sistema informativo

Si riportano nel seguito le sintesi delle e-competence con i relativi livelli

A.7. Osservatorio Tecnologico Esplora gli ultimi sviluppi tecnologici dell'ICT per comprenderne l'evoluzione tecnologica. Concepisce soluzioni innovative per l'integrazione di nuove tecnologie nei prodotti, applicazioni e servizi esistenti o per la creazione di nuove soluzioni.	Livello 4
D.1. Sviluppo della Strategia della Sicurezza Informatica Definisce e rende applicabile formalmente la strategia, gli obiettivi e la cultura organizzativa al fine di mantenere la sicurezza e la difesa dei dati. Fornisce la base per la gestione della Sicurezza dell'informazione, compresa l'identificazione dei ruoli e delle responsabilità (ref D.2). Usa gli standard definiti per determinare gli obiettivi per l'integrità, la disponibilità e la privacy delle informazioni.	Livello 5
E.3. Gestione del Rischio Implementa la gestione del rischio dei sistemi informativi attraverso l'applicazione delle politiche e procedure definite dall'azienda per la gestione del rischio. Valuta il rischio per il business dell'organizzazione e documenta rischi potenziali e piani di prevenzione.	Livello 3
E.9. IT Governance Definisce, realizza e controlla la gestione dei sistemi informativi in linea con i vincoli di business. Tiene conto di tutti i parametri interni ed esterni come la normativa e l'aderenza agli standard industriali per indirizzare la gestione del rischio e dell'impiego delle risorse al fine di raggiungere i benefici di business messi a bilancio.	Livello 4
E.8. Gestione della Sicurezza dell'Informazione Implementa la politica della sicurezza dell'informazione. Controlla e prende iniziative a fronte di intrusioni, frodi e buchi o falle della sicurezza. Assicura che i rischi legati alla sicurezza siano analizzati e gestiti per i dati e le informazioni aziendali. Rivede gli incidenti sulla sicurezza e fornisce raccomandazioni per un miglioramento continuo della sicurezza.	Livello 4

2.3.6 Formazione Professionale (non formale)

non sono previsti requisiti di formazione per l'accesso all'esame.

2.3.7 Esperienza professionale

10 anni di esperienza professionale nella sicurezza informatica di cui 2 come manager negli ultimi 3 anni.

3. ESAME DI CERTIFICAZIONE

3.1 Programma Delle Prove

Il programma delle prove si compone di 3 tipologie di prove:

1. 1 prova scritta a risposte chiuse;
2. 1 prova scritta su scenari;
3. prova orale.

Tabella indicativa delle attività e del programma delle prove

Orario	Attività
9.00	Identificazione candidati
10.00	Presentazione Esame, Programma delle Prove, Criteri di valutazione, Modulistica d'esame, procedura di segnalazione ricorsi e reclami.
10.30	Consegna ed Esecuzione della prima prova scritta
11.30	Consegna ed Esecuzione della seconda prova scritta
12.30	Correzione degli elaborati e preparazione calendario prove orali
13.30	pausa ristoro
14.00	Avvio prove orali – (ipotesi 20 min a candidato)
18.30	Redazione Verbale finale

3.2 Descrizione e criteri di valutazione delle Prove

La commissione può modificare la sequenza delle prove scritte, mentre la prova orale risulterà comunque essere l'ultima.

- **Prima Prova Scritta**

La prima prova scritta di compone di 20 domande a risposta chiusa, con 4 alternative, fra le quali solo una è quella esatta.

Il candidato deve evidenziare la risposta per lui corretta, ciascuna risposta corretta vale un punto, quelle sbagliate o non date valgono 0 punti, non si assegnano punteggi negativi.

La sufficienza sulla tale prova viene raggiunta totalizzando il 70% di risposte corrette (7/10 di risposte corrette).

- **Seconda Prova Scritta**

La seconda prova scritta consiste in uno scenario professionale descritto in lingua inglese che può vertere su interpretazioni, normativa applicabile, azioni da intraprendere.

La correzione della prova viene eseguita a fronte di griglie di valutazione che implementano le risposte ammissibili e le casistiche approvate. La commissione valuta le risposte del candidato sulla base delle indicazioni definite dalla griglia di riferimento.

Il candidato viene ammesso alla prova orale se, oltre ad aver ottenuto almeno il 70% di risposte esatte nella prima prova scritta, ottiene una media delle due prove scritte pari almeno al 60% (60/100).

- **Prova Orale**

L'Esaminatore sottopone al candidato un numero adeguato di domande (consigliato 4) che sono valutate su base 100. Per ogni domanda il punteggio varia da 0 a 100, per il calcolo del punteggio finale si effettua la media fra tutte le risposte.

Nella conduzione delle prove orali gli esaminatori devono verificare le Competenze Professionali dei candidati, sono quindi consigliate domande aperte nelle quali offrire al candidato la possibilità di illustrare uno scenario professionale con le possibili soluzioni.

L'Esaminatore può partire dalla prova scritta o pratica per approfondire un tema particolarmente importante o sul quale il candidato abbia mostrato carenza, le domande devono garantire, per quanto possibile, un ampio spettro di indagine sull'intera gamma dei requisiti

Tabella valutazione prova orale

Valore	Ambito	Giudizio
0-19	**Comprensione domanda**	Il candidato non ha compreso la domanda
	Appropriatezza risposta	La risposta è assente o non è pertinente all'ambito della domanda. Il candidato mostra assenza di padronanza dell'argomento
20-39	**Comprensione domanda**	Il candidato ha compreso parzialmente la domanda
	Appropriatezza risposta	La risposta è generica e non soddisfacente o non completamente pertinente. Il candidato mostra assenza di padronanza dell'argomento
40-59	**Comprensione domanda**	Il candidato ha compreso la domanda
	Appropriatezza risposta	La risposta pur essendo appropriata è incompleta o incerta. Il candidato mostra una certa padronanza dell'argomento non ancora sufficiente
60-79	**Comprensione domanda**	Il candidato ha compreso pienamente la domanda
	Appropriatezza risposta	La risposta è completa ma non dettagliata. Il candidato mostra sufficiente padronanza dell'argomento.
80-100	**Comprensione domanda**	Il candidato ha compreso la domanda dando prova di una comprensione globale negli aspetti professionali collegati
	Appropriatezza risposta	La risposta è completa e dettagliata. Il candidato mostra ottima padronanza dell'argomento.

Il Punteggio Finale (**PF**) viene calcolato con la seguente formula:

PF = 0,30*PS1 + 0,30*PS2 +0,40*PO

dove PS1 è il punteggio in centesimi della prima prova scritta, PS2 è il punteggio in centesimi della seconda prova scritta e PO è il punteggio in centesimi della prova orale.

- **Valutazione Complessiva delle prove**

La prova scritta e la prova orale, devono raggiungere il punteggio del 70% di risposte esatte. Per superare l'esame complessivo, la valutazione totale delle prove (scritto e orale) dovrà essere pari al 70% di risposte esatte totali.

Al termine della valutazione complessiva del candidato, la commissione lo informa dell'esito dell'esame, ricordando che se l'esito è risultato positivo, la delibera di certificazione finale spetta al Deliberatore nominato da Kiwa Cermet.

Il candidato che non ha superato la prova d'esame, può ripeterla entro cinque (5) mesi, pagando la solo quota relativa all'esecuzione dell'esame.

4. SORVEGLIANZA E RINNOVO

4.1 Requisiti per il Mantenimento della certificazione

La durata della certificazione è stabilità in cinque anni dalla data di delibera del certificato, **annualmente** il professionista certificato deve produrre e trasmettere a Kiwa Cermet:

- Evidenza dell'esercizio retribuito della professione;
- Evidenza dell'aggiornamento professionale eseguito nella misura di 30 crediti annuali (1 credito = 1 ora di formazione);
- Evidenze della registrazione e del trattamento dei reclami ricevuti;
- Evidenza del pagamento della quota annuale così come indicato nel tariffario di schema.

Tali evidenze potranno essere prodotte con una autodichiarazione ai sensi del DPR 445 del 28/12/2000, in tal caso le evidenze potranno essere verificate da funzionari Kiwa Cermet debitamente incaricati al controllo della documentazione professionale. Come evidenze dei crediti formativi richiesti saranno ritenute valide anche le dichiarazioni rilasciate dalle Associazioni Professionali del settore, che operano conformemente a quanto previsto dalla legge 4 del 14/01/2013 e risultano iscritte nell'apposito elenco delle associazioni delle professioni non regolamentate, pubblicato dal Ministero della Giustizia.

4.2 Requisiti per il rinnovo quinquennale della certificazione

Alla scadenza del quinquennio di certificazione il professionista certificato deve dare:

- Evidenza dell'esercizio retribuito della professione;
- Evidenza della formazione nella misura di 150 crediti (totale del triennio);
- Evidenze della registrazione e del trattamento dei reclami ricevuti;
- Evidenza del pagamento della quota annuali come previsto nel tariffario di schema.

Le evidenze devono essere supportate da documentazione di corredo che mostri e attesti l'effettivo soddisfacimento del requisito. Come evidenze dei crediti formativi richiesti saranno ritenute valide anche le dichiarazioni rilasciate dalle Associazioni Professionali del settore, che operano conformemente a quanto previsto dalla legge 4 del 14/01/2013 e risultano iscritte nell'apposito elenco delle associazioni delle professioni non regolamentate, pubblicato dal Ministero della Giustizia.

Se nel periodo di validità della certificazione, mutate condizioni del contesto lavorativo, professionale o normativo impongono una revisione del profilo professionale, la Direzione Certificazione comunicherà le variazioni e le eventuali disposizioni per il mantenimento della certificazione.