STATO DELLE REVISIONI		
rev. n°	SINTESI DELLA MODIFICA	DATA
4	Adeguamento all'edizione 2017 della Norma UNI 11506	2018-04-10
3	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 Specialist.**

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 Specialist (UNI 11621-2 – profilo n°12)

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 Specialist (specialista DELLA SICUREZZA ICT)**		
Descrizione sintetica	Assicura l'implementazione della politica di sicurezza aziendale.		
Missione	Propone ed implementa I necessari aggiornamenti della sicurezza. Consiglia, supporta, informa e fornisce addestramento e consapevolezza sulla sicurezza. Conduce azioni dirette su tutta o parte di una rete o di un sistema. E' riconosciuto come l'esperto tecnico della sicurezza ICT dai colleghi.		
Deliverable	**Accountable**	**Responsible**	**Contributor**
	• Base di conoscenza o informazione (Sicurezza)	• Proposta integrazione nuove tecnologie (Sicurezza)	• Politica di gestione dei rischi • Piano gestione dei rischi • Politica sicurezza informazioni
Task principali	• Assicura la sicurezza e l'uso appropriato delle risorse ICT • Valuta rischi, minacce e conseguenze • Fornisce addestramento e formazione sulla sicurezza • Provvede alla validazione tecnica dei tool di sicurezza • Contribuisce alla definizione degli standard di sicurezza • Controlla la vulnerabilità della sicurezza • Controlla gli sviluppi della sicurezza per assicurare la sicurezza fisica e dei dati delle risorse ICT		
e-competence *(da e-CF)*	C.2. Supporto al cambiamento		Livello 3
	C.3. Erogazione del servizio		Livello 3
	D.9. Sviluppo del Personale		Livello 3
	D.10. Gestione dell'Informazione e della Conoscenza		Livello 3
	E.8. Gestione della Sicurezza dell'Informazione		Livello 3-4
Area di applicazione dei KPI	Misure di Sicurezza adottate		

2.2.1 Dettaglio e-competenze secondo CWA 16234 parte I

ICT SECURITY Specialist (specialista DELLA SICUREZZA ICT)		
Dimensione 2 – e-competence **Dimensione 3 – livelli di abilità**	**Dimensione 4 – knowledge** **Conosce/ E' informato su/ Ha familiarità con;**	**Dimensione 4 – skill** **E' capace di;**
C. RUN (ESERCIRE)		
C.2. Supporto al Cambiamento (Change Support) Implementa e fornisce assistenza per l'evoluzione di una soluzione IT. Controlla e schedula in modo efficiente le modifiche software o hardware per prevenire aggiornamenti multipli che creano esiti imprevedibili. Minimizza le interruzioni del servizio conseguenti ai cambiamenti e aderisce ai service level agreement (SLA) definiti.	• K1 le specifiche funzionali di un sistema informativo • K2 l'architettura tecnica di un'applicazione ICT esistente • K3 come i processi business sono integrati e la loro dipendenza dalle applicazioni ICT • K4 strumenti e tecniche per la gestione del cambiamento	• S1 condividere specifiche funzionali e tecniche con i team ICT che hanno in carico la manutenzione e l'evoluzione delle soluzioni ICT • S2 gestire le comunicazioni con i team che hanno in carico la manutenzione e l'evoluzione dei sistemi informativi. • S3 analizzare l'impatto sugli utenti dei cambiamenti funzionali/tecnici • S4 anticipare tutte le azioni necessarie a mitigare l'impatto dei cambiamenti (formazione, documentazione, nuovi processi...)
Livello 2 – Durante il cambiamento, opera sistematicamente per rispondere alle necessità operative quotidiane e reagisce a queste evitando interruzioni di servizio e mantenendo la coerenza con il service level agreement (SLA).		
Livello 3 – Assicura l'integrità del sistema controllando l'applicazione degli aggiornamenti funzionali, l'aggiunta di software o hardware e le attività di manutenzione. E' conforme ai requisiti di budget.		
C. RUN (ESERCIRE)		
C.3. Erogazione del Servizio (Service Delivery) Opera in modo proattivo per garantire un'infrastruttura applicativa e ICT stabile e sicura. Aggiorna la libreria dei documenti di esercizio e registra tutti gli eventi di esercizio. Cura la manutenzione degli strumenti di monitoraggio e di gestione (es. Scripts, Procedure...).	• K1 come interpretare i requisiti di erogazione dei servizi ICT • K2 le best practice e gli standard relativi all'erogazione di servizi ICT • K3 come monitorare la erogazione del servizio • K4 come registrare le attività relative all'erogazione del servizio ed è capace ad identificare i guasti	• S1 applicare i processi che includono l'organizzazione strategica della erogazione del servizio ICT • S2 compilare e completare la documentazione usata nella erogazione del servizio ICT • S3 analizzare l'erogazione del servizio disponibile e produrre il report dei risultati ai colleghi superiori
Livello 1 – Opera sotto controllo per registrare dati inerenti l'affidabilità		
Livello 2 – Analizza sistematicamente i dati di prestazione e comunica le conclusioni agli esperti senior. Scala le carenze nei livelli potenziali di servizio e raccomanda azioni per migliorare l'affidabilità del servizio. Traccia i dati di affidabilità confrontandoli con il service level agreement		
Livello 3 – Programma la schedulazione delle attività operative. Gestisce i costi e il budget in accordo con le procedure interne ed i vincoli esterni. Identifica i requisiti delle risorse necessarie alla gestione operativa dell'infrastruttura ICT		

ICT SECURITY Specialist (specialista DELLA SICUREZZA ICT)		
Dimensione 2 – e-competence Dimensione 3 – livelli di abilità	**Dimensione 4 – knowledge Conosce/ E' informato su/ Ha familiarità con;**	**Dimensione 4 – skill E' capace di;**
D.ENABLE (ABILITARE)		
D.9 Sviluppo del Personale (Personnel Development) Diagnostica le competenze individuali e di gruppo, identificando gli skill necessari e gli skill gaps. Esamina le opzioni di formazione e sviluppo e seleziona l'appropriata metodologia tenendo conto delle necessità degli individui e del business. Prepara e/o addestra individui e team per indirizzare i fabbisogni di apprendimento	• K1 i metodi di sviluppo delle competenze • K2 le metodologie di analisi dei fabbisogni di competenze e skill • K3 i metodi a supporto dell'apprendimento e dello sviluppo (es. coaching, insegnamento) • K4 ICT le tecnologie e i processi con una prospettiva d'insieme	• S1 identificare gap di competenze e skill gap • S2 identificare e raccomandare opportunità di sviluppo basate sulla pratica lavorativa • S3 incorporare nei processi di lavoro quotidiani le opportunità di sviluppo degli skill • S4 offrire supporto sui processi di apprendimento
Livello 2 – Informa/forma individui e gruppi, tiene corsi di istruzione		
Livello 3 – Monitora e indirizza i fabbisogni di sviluppo degli individui e dei team.		
Livello 4 – Agisce in modo proattivo e sviluppa processi organizzativi per indirizzare i fabbisogni di sviluppo di individui, gruppi o dell'intera forza lavoro.		
D.ENABLE (ABILITARE)		
D.10 Gestione dell'Informazione e della Conoscenza (Information and Knowledge Management) Identifica e gestisce informazioni strutturate e non strutturate e considera le politiche sulla distribuzione dell'informazione. Crea la struttura delle informazioni per abilitare l'impiego e l'ottimizzazione dell'informazione finalizzati ai benefici del business. Comprende gli strumenti appropriati che devono essere diffusi per creare, estrarre, mantenere, rinnovare e diffondere la conoscenza del business al fine di capitalizzare il patrimonio informativo.	• K1 i metodi per analizzare le informazioni non strutturate e i processi di business • K2 gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero dei dati	• S1 raccogliere la conoscenza interna ed sterna e i fabbisogni di informazione • S2 formalizzare i requisiti del cliente • S3 tradurre/ riflettere il comportamento del business in informazione strutturata • S4 rendere l'informazione disponibile
Livello 3 – Analizza i processi del Business e i requisiti dell'informazione associati e rende disponibile la struttura dell'informazione più appropriata.		
Livello 4 – Integra la struttura delle informazioni appropriata nell'ambiente organizzativo.		
Livello 5 – Correla informazioni e conoscenza per creare valore per il business. Applica soluzioni innovative basate sulle informazioni recuperate.		
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	• 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	• 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

ICT SECURITY Specialist (specialista DELLA SICUREZZA ICT)		
Dimensione 2 – e-competence Dimensione 3 – livelli di abilità	**Dimensione 4 – knowledge Conosce/ E' informato su/ Ha familiarità con;**	**Dimensione 4 – skill E' capace di;**
analizzati e gestiti per i dati e le informazioni aziendali. Rivede gli incidenti sulla sicurezza e fornisce raccomandazioni per un miglioramento continuo della sicurezza.	• K3 I rischi critici per la gestione della sicurezza • K4 l'approccio all'attività ispettiva interna del sistema informativo	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.		
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		

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 Triennale o 5 Anni di esperienza nel settore della 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 (requisiti 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 specifiche funzionali di un sistema informativo • l'architettura tecnica di un'applicazione ICT esistente • come i processi business sono integrati e la loro dipendenza dalle applicazioni ICT • strumenti e tecniche per la gestione del cambiamento
• come interpretare i requisiti di erogazione dei servizi ICT • le best practice e gli standard relativi all'erogazione di servizi ICT • come monitorare la erogazione del servizio • come registrare le attività relative all'erogazione del servizio ed è capace ad identificare i guasti
• i metodi di sviluppo delle competenze • le metodologie di analisi dei fabbisogni di competenze e skill • i metodi a supporto dell'apprendimento e dello sviluppo (es. coaching, insegnamento) • ICT le tecnologie e i processi con una prospettiva d'insieme
• i metodi per analizzare le informazioni non strutturate e i processi di business • gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero dei dati
• 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

2.3.5 Competenze Tecnico-Professionali specialistiche

É capace di:
• condividere specifiche funzionali e tecniche con i team ICT che hanno in carico la manutenzione e l'evoluzione delle soluzioni ICT • gestire le comunicazioni con i team che hanno in carico la manutenzione e l'evoluzione dei sistemi informativi. • analizzare l'impatto sugli utenti dei cambiamenti funzionali/tecnici • anticipare tutte le azioni necessarie a mitigare l'impatto dei cambiamenti (formazione, documentazione, nuovi processi...)
• applicare i processi che includono l'organizzazione strategica della erogazione del servizio ICT • compilare e completare la documentazione usata nella erogazione del servizio ICT • analizzare l'erogazione del servizio disponibile e produrre il report dei risultati ai colleghi superiori
• identificare gap di competenze e skill gap • identificare e raccomandare opportunità di sviluppo basate sulla pratica lavorativa • incorporare nei processi di lavoro quotidiani le opportunità di sviluppo degli skill • offrire supporto sui processi di apprendimento
• raccogliere la conoscenza interna ed sterna e i fabbisogni di informazione • formalizzare i requisiti del cliente • tradurre/ riflettere il comportamento del business in informazione strutturata • rendere l'informazione disponibile
• 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

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

C.2. Supporto al Cambiamento (Change Support) Implementa e fornisce assistenza per l'evoluzione di una soluzione IT. Controlla e schedula in modo efficiente le modifiche software o hardware per prevenire aggiornamenti multipli che creano esiti imprevedibili. Minimizza le interruzioni del servizio conseguenti ai cambiamenti e aderisce ai service level agreement (SLA) definiti.	Livello 3
C.3. Erogazione del Servizio (Service Delivery) Opera in modo proattivo per garantire un'infrastruttura applicativa e ICT stabile e sicura. Aggiorna la libreria dei documenti di esercizio e registra tutti gli eventi di esercizio. Cura la manutenzione degli strumenti di monitoraggio e di gestione (es. Scripts, Procedure...).	Livello 3
D.9 Sviluppo del Personale (Personnel Development) Diagnostica le competenze individuali e di gruppo, identificando gli skill necessari e gli skill gaps. Esamina le opzioni di formazione e sviluppo e seleziona l'appropriata metodologia tenendo conto delle necessità degli individui e del business. Prepara e/o addestra individui e team per indirizzare i fabbisogni di apprendimento	Livello 3
D.10 Gestione dell'Informazione e della Conoscenza (Information and Knowledge Management) Identifica e gestisce informazioni strutturate e non strutturate e considera le politiche sulla distribuzione dell'informazione. Crea la struttura delle informazioni per abilitare l'impiego e l'ottimizzazione dell'informazione finalizzati ai benefici del business. Comprende gli strumenti appropriati che devono essere diffusi per creare, estrarre, mantenere, rinnovare e diffondere la conoscenza del business al fine di capitalizzare il patrimonio informativo.	Livello 3
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.	Livello 3-4

2.3.6 Formazione Professionale (non formale)

Non sono previsti requisiti di formazione per accesso all'esame.

2.3.7 Esperienza professionale

Tre anni come specialista nella sicurezza informatica.

3. ESAME DI CERTIFICAZIONE

3.1 Programma Delle Prove

Il programma delle prove si compone di 2 tipologie di prove:
1. 1 prova scritta a risposte chiuse;
2. 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 prova scritta
11.30	Correzione degli elaborati e preparazione calendario prove orali
12.30	pausa ristoro
13.30	Avvio prove orali – (ipotesi 20 min a candidato)
18.00	Redazione Verbale finale

3.2 Descrizione e criteri di valutazione delle Prove

- **Prova Scritta**

La prova scritta si compone di 30 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, le risposte sbagliate valgono 0 punti, non si assegnano punteggi negativi.

La sufficienza della prova scritta viene raggiunta totalizzando il 70% di risposte esatte.

Il candidato viene ammesso alla prova orale, solo se ha superato la prova scritta.

- **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. Il punteggio della prova orale deve risultare superiore o uguale a **60/100** per essere dichiarata positiva.

Il punteggio finale viene calcolato con la media dei punteggi ottenuti nelle prove scritta e orale, il candidato che ha totalizzato punteggio inferiore a **70/100** non prosegue nell'iter di certificazione.

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 per approfondire un tema particolarmente importante, o rispetto al quale il candidato abbia mostrato delle carenze, 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 ma 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.

- **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 del pagamento della quota annuale così come indicato nel tariffario;
- Evidenza dell'esercizio retribuito della professione;
- Evidenza dell'aggiornamento professionale eseguito nella misura di **10 crediti** annuali (1 credito = 1 ora di formazione);
- Evidenze della registrazione e del trattamento dei reclami ricevuti.

Tali evidenze potranno essere prodotte con un'autodichiarazione ai sensi del DPR 445 del 28/12/2000, in tal caso le evidenze potranno essere verificate da funzionari Kiwa Cermet debitamente incaricati alla 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.

2.2 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 **50 crediti** (totale del quinquennio);
- Evidenze della registrazione e del trattamento dei reclami ricevuti;
- Evidenza del pagamento della quota annuali come previsto dal 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, il Direttore di Divisione comunicherà le variazioni e le eventuali disposizioni per il mantenimento della certificazione.