Schema per Information Security Specialist

LISTA REVISIONI

Rev.	Data	Descrizione	Redazione	Verifica	Approvazione
Rev. 3	17/01/2023	Revisione con aggiornamento maggio 2021 di UNI11506 e UNI11621-2	Resp. Schema	Direttore	Amministratore

INDICE

Sommario

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce i requisiti e le modalità per la certificazione delle competenze dei candidati per il profilo professionale di **Information Security Specialist**.
Il documento, sviluppato da Istituto Volta S.r.l., definisce una SCHEMA DI CERTIFICAZIONE che viene gestito dallo stesso Organismo per regolamentare il processo di Certificazione di figure professionali e per il mantenimento della certificazione nel suo periodo di validità.
Lo scopo finale della certificazione di persone consiste, attraverso un processo di valutazione affidabile ed imparziale, nel riconoscere la competenza di una singola persona per eseguire un compito o un lavoro. L'istituto VOLTA S.r.l., nel processo di certificazione, garantisce la massima imparzialità ed indipendenza nei confronti dei professionisti.
Il presente documento, d'ora in avanti definito più brevemente Schema, definisce, in maniera dettagliata ed esauriente, i requisiti, il processo di certificazione, le modalità di iscrizione al registro dei professionisti certificati, il rilascio della certificazione, le modalità e le prassi per il mantenimento della certificazione, i possibili provvedimenti disciplinari e le conseguenti sanzioni, le modalità di sorveglianza e rinnovo della certificazione, le modalità di gestione dei reclami e dei ricorsi.
Il presente Schema si applica sia ai neo Candidati che abbiano presentato domande di certificazione sia a persone già certificate e già iscritte nell'apposito Registro.

2. DOCUMENTI DI RIFERIMENTO

- UNI CEI EN ISO/IEC 17024:2012 "Requisiti generali per gli organismi che eseguono la certificazione delle persone"
- UNI 11506:2021 "Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Requisiti per la valutazione della conformità delle conoscenze, abilità, autonomia e responsabilità per i profili professionali ICT basati sul modello e-CF"
- UNI 11621-2:2021 Attività professionali non regolamentate – Profili professionali per l'ICT – Parte 2: Profili professionali di "seconda generazione". *Contiene i profili professionali ICT di seconda generazione (23 profili professionali, compresa la figura oggetto del presente schema)*
- UNI EN 16234-1:2020 "e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework". Contiene il framework per la definizione delle competenze ICT specialistiche (e-Competence Framework 3.0).
- CWA 16234 part.1 (Schema e-CF) "e-Competence Framework Europeo – Framework comune europeo per i professionisti ICT in tutti i settori industriali"
- CWA 16458:2018 (tutte le parti) "European ICT professionals role profiles"
- Regolamento (UE) n. 1025/2012 del Parlamento Europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio
- Lg. 04/2013 "Disposizioni in materia di professioni non organizzate in ordini e collegi"
- D. Lgs13/2013 "Definizione delle norme generali e dei livelli essenziali delle prestazioni per l'individuazione e validazione degli apprendimenti non formali e informali e degli standard minimi di servizio del sistema nazionale di certificazione delle competenze, a norma dell'articolo 4, commi 58 e 68, della legge 28 giugno 2012, n. 92"
- Raccomandazione del Consiglio del 22 maggio 2017 sul Quadro europeo delle qualifiche per l'apprendimento permanente, che abroga la raccomandazione del Parlamento europeo e del Consiglio, del 23 aprile 2008, sulla costituzione del quadro europeo delle qualifiche per l'apprendimento permanente (2017/C 189/03).

I documenti citati rappresentano i principali riferimenti normativi e legislativi del settore e sono applicabili nell'ultima edizione valida.

3. TERMINI E DEFINIZIONI

- Candidato: richiedente che possiede i prerequisiti specificati ed è stato ammesso al processo di certificazione
- Esaminatore: persona che ha la competenza per condurre un esame e, ove tale esame richieda un giudizio professionale, valutarne i risultati
- Esame: attività che fanno parte della valutazione, che permettono di misurare la competenza di un candidato mediante uno o più mezzi quali prove scritte, orali, pratiche od osservazione diretta
- Valutazione: Processo che permette di valutare se una persona possiede i requisiti dello schema di certificazione.

4. PROFILO DELLA FIGURA PROFESSIONALE

Il presente schema di certificazione definisce il processo di certificazione in conformità alla norma UNI CEI EN ISO/IEC 17024:2012. Lo schema di certificazione rimanda inoltre alla norma UNI 11621-2:2021 nel profilo di seconda generazione dell'INFORMATION SECURITY SPECIALIST.

Le norme citate definiscono i requisiti relativi all'attività del professionista ICT e delle diverse figure che operano in tale ambito (tra cui, il Security Specialist), indipendentemente dalle modalità lavorative e dalla tipologia del rapporto di lavoro, stabilendo le prerogative fondamentali per l'insieme di conoscenze, abilità e competenze che le contraddistinguono. Vengono inoltre chiarite le metodologie con le quali descrivere tale professionalità.

Coerentemente alle peculiarità del settore informatico (ambito in continua evoluzione in cui nascono costantemente nuove aree, nuove tecnologie, nuove professionalità) la norma applicabile non entra nel merito delle singole professioni ma presenta uno spettro d'azione molto ampio: definisce, infatti, 40 tipi di competenze generali che sono di riferimento per tutta l'area ICT.

In dettaglio, la norma UNI EN 16234-1:2020 offre una definizione chiara ed una guida sicura a supporto delle decisioni sia nel processo di selezione e reclutamento dei candidati, sia in quello di assessment e formazione di professionisti ICT.

L' e-Competence Framework 3.0 (UNI EN 16234-1:2020) è strutturato in quattro dimensioni. Queste dimensioni riflettono differenti livelli di requisiti di business e di pianificazione delle risorse umane e integrano delle linee guida per la definizione dei livelli di abilità lavorative. Le dimensioni sono così strutturate:

• Dimensione 1: 5 aree di e-Competence, derivate dai processi business dell'ICT: A. PLAN (PIANIFICARE) – B. BUILD (REALIZZARE) – C. RUN (OPERARE) – D. ENABLE (ABILITARE) – E. MANAGE (GESTIRE).

• Dimensione 2: Un insieme di e-Competence di riferimento per ciascuna area, con una descrizione generica per ciascuna competenza. Le 40 competenze identificate in totale forniscono le definizioni di riferimento dell'e-CF 3.0.

• Dimensione 3: Livelli di Capacità per ciascuna e-Competence: sono articolati in Livello di e-Competence da e-1 a e-5, e messi in relazione con i livelli EQF da 3 a 8.

• Dimensione 4: Esempi di knowledge (conoscenza) e skill (capacità): sono in relazione alla dimensione 2 della e-Competence. Tali esempi, descrivono il contesto aggiungendo valore al framework e comunque non devono ritenersi esaustivi.

Di seguito un prospetto con la visione di insieme della European e-Competence Framework versione 3.0.

Dimensione 1 5 aree e-CF	Dimensione 2 40 e-Competences identificate	Dimensione 3 Livelli di Capacità – livelli da e-1 a e-5, collegati ai livelli EQF 3–8				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. Allineamento Strategie IS e di Business				■	■
	A.2. Gestione dei Livelli di Servizio			■	■	
	A.3. Sviluppo del Business Plan			■	■	■
	A.4. Pianificazione di Prodotto o di Servizio		■	■	■	
	A.5. Progettazione di Architetture			■	■	■
	A.6. Progettazione di Applicazioni	■	■	■		
	A.7. Monitoraggio dei Trend tecnologici				■	■
	A.8. Sviluppo Sostenibile			■	■	
	A.9. Innovazione				■	■
B. BUILD	B.1. Sviluppo di Applicazioni	■	■	■		
	B.2. Integrazione dei Componenti		■	■	■	
	B.3. Testing	■	■	■	■	
	B.4. Rilascio (deployment) della Soluzione	■	■	■		
	B.5. Produzione della Documentazione	■	■	■		
	B.6. Ingegneria dei Sistemi			■	■	
C. RUN	C.1. Assistenza all'Utente	■	■	■		
	C.2. Supporto alle modifiche/evoluzioni del Sistema		■	■		
	C.3. Erogazione del Servizio	■	■	■		
	C.4. Gestione del Problema		■	■	■	
D. ENABLE	D.1. Sviluppo della Strategia per la Sicurezza Informatica				■	■
	D.2. Sviluppo della Strategia della Qualità ICT				■	■
	D.3. Fornitura dei servizi di Formazione		■	■		
	D.4. Acquisti		■	■	■	
	D.5. Sviluppo dell'Offerta		■	■		
	D.6. Gestione del Canale di Vendita			■	■	
	D.7. Gestione delle Vendite			■	■	■
	D.8. Gestione del Contratto		■	■	■	
	D.9. Sviluppo del Personale		■	■	■	
	D.10. Gestione dell'Informazione e della Conoscenza			■	■	■
	D.11. Identificazione dei Fabbisogni			■	■	■
	D.12. Marketing Digitale		■	■	■	
E. MANAGE	E.1. Formulazione delle Previsioni			■	■	
	E.2. Gestione del Progetto e del Portfolio		■	■	■	■
	E.3. Gestione del Rischio		■	■	■	
	E.4. Gestione delle Relazioni			■	■	
	E.5. Miglioramento del Processo			■	■	
	E.6. Gestione della Qualità ICT		■	■	■	
	E.7. Gestione del Cambiamento del Business			■	■	■
	E.8. Gestione della Sicurezza dell'Informazione		■	■	■	
	E.9. IS Governance				■	■

4.1 Tabella di corrispondenza livelli e-CF e EQF

La norma "e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors" fornisce un riferimento comune per 40 profili professionali nel settore dell'Information and Communication Technology (ICT), utilizzando un linguaggio comune che può essere compreso in tutta Europa per definire le competenze, le capacità e i livelli di preparazione di questi profili.
Il livello di istruzione (formazione formale) è stato assegnato sulla base della letteratura in materia comunemente adottata dato che comunque il sistema EQF ed e-CF non identificano una scolarità, ma un livello di conoscenze, abilità e competenze indipendentemente dal titolo di studio, dato che fa parte della formazione anche la formazione informale ovvero l'apprendimento avvenuto attraverso l'esperienza lavorativa.
Per una corretta interpretazione si riporta lo schema specifico dei livelli e-CF e il parallelo ai livelli EQF.

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)

4.2 Descrizione del profilo

Titolo del Profilo	**INFORMATION SECURITY SPECIALIST**		
Descrizione sintetica	Figura professionale che garantisce l'implementazione della politica di sicurezza delle informazioni dell'organizzazione attraverso l'uso sicuro e appropriato delle risorse ICT.		
Missione	Il Security Specialist definisce, propone e implementa le tecniche e le pratiche di sicurezza delle informazioni necessarie in conformità con gli standard e le procedure di sicurezza delle informazioni. Contribuisce alle pratiche di sicurezza, consapevolezza e conformità fornendo consulenza, supporto, informazione e formazione.		
Deliverable	**Responsible (R)**	**Accountable (A)**	**Contributor (C)**
	Conoscenza o base di informazioni (Sicurezza)	Soluzione e proposta di integrazione dei processi aziendali critici (Sicurezza) Valutazione del rischio per la sicurezza delle informazioni	Politica di gestione dei rischi Piano gestione dei rischi per la sicurezza delle informazioni Politica di sicurezza delle informazioni
Task principali	- Valutare i rischi, le minacce e le conseguenze sulla sicurezza delle informazioni e adottare le misure appropriate - Fornire formazione e istruzione sulla sicurezza delle informazioni - Fornire la convalida tecnica degli strumenti di sicurezza, implementare, configurare e gestire strumenti appropriati - Contribuire alla definizione e promuovere attivamente gli standard e le procedure di sicurezza delle informazioni attraverso l'IT e nelle comunità di utenti IT - Identificare e correggere le vulnerabilità della sicurezza - Monitorare gli sviluppi della sicurezza per garantire la continua efficienza ed efficacia dei processi e dei controlli di sicurezza delle informazioni - Valutare in modo proattivo nuove minacce e contrastare potenziali incidenti di sicurezza delle informazioni - Implementare tecniche di sicurezza su tutta o parte di un'applicazione, processo, rete o sistema all'interno dell'area di responsabilità		
e-competence (dimensione 2 e dimensione 3 dell'e-CF)	• **A.7** Monitoraggio delle tendenze tecnologiche		Livello 4
	• **A.9** Innovazione		Livello 4
	• **D.1** Sviluppo della strategia per la Sicurezza Informatica		Livello 4
	• **D.3** Fornitura dei servizi di formazione		Livello 3
	• **E.3** Gestione del rischio		Livello 3
Area di applicazione dei KPI	Misure di Sicurezza in atto		

Nel caso specifico del presente schema, il livello medio e-CF è pari a: 4.

4.3 Dettaglio delle Conoscenze, delle Abilità e delle Competenze

La descrizione delle Abilità, Conoscenze e competenze di base, Trasversali e Tecnico Professionali oggetto dell'esame è in UNI EN 16234-1:2020.

Coloro che sono interessati a candidarsi per la certificazione del Security Specialist possono verificare le competenze che essi devono saper dimostrare di possedere durante l'esame, consultando il Modello e-CF 3.0 (UNI EN 16234-1:2020), selezionando tra le 40 e-competence indicate in "dimensione 2" quelle specifiche del profilo del presente schema (**A7 – A9 – D1 – D3 – E3**).

5. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEL SECURITY SPECIALIST

Possono accedere all'esame i richiedenti che siano in possesso dei prerequisiti riportati nei paragrafi successivi.

L'accesso alla prova di valutazione è subordinato all'invio di una richiesta di certificazione da parte del candidato all'Istituto Volta, Organismo di Certificazione che effettua la valutazione.

I criteri di definizione dei pre-requisiti di accesso adottati sono derivati da quanto espresso in UNI 11506:2021 all'Appendice A.2 "Elementi per l'accesso al processo di valutazione della conformità (Esame di certificazione)".

5.1 Idoneità

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

5.2 Formazione Formale, non formale e Informale

5.2.1 Formale

- Media dei livelli di e-competence richiesti (tratti da e-CF 3.0), così come illustrati al precedente punto 4.2 "Descrizione del profilo"; con tale media si determina il livello e-CF per lo specifico profilo.
- Riscontro del livello di formazione formale (istruzione) definito nella tabella comparativa e-CF / EQF riportata in questo documento al punto 4.1 "Tabella di corrispondenza livelli e-CF e EQF".

Si precisa che la comparazione e-CF/EQF riportata nei documenti pubblicati in e-CF non prevede un titolo di studio, bensì competenza. In assenza di una norma che prescriva la correlazione standard tra titolo di studio e livello EQF, si adotta la tabella citata al punto 4.1 di questo documento; è ammessa comunque la equipollenza tra Laurea Magistrale (formazione formale) e formazione informale con esperienza di almeno 4 anni nel settore informatico di cui almeno 3 in ruolo. Per laurea magistrale specialistica, il numero minimo di anni richiesti nel ruolo è ridotto di -1 anno.

5.2.2 Non formale

Si richiede al candidato di dimostrare il conseguimento di un numero minimo di crediti negli ultimi 12 mesi. Nel caso della presente figura (livello medio e-CF 4), i crediti devono essere n. 8, pari a 8 ore di formazione.

5.2.3 Informale

In base a quanto previsto dalla norma UNI 11506:2021, in corrispondenza a valori di e-competence media determinati per lo specifico profilo corrispondenti ai livelli e-CF, si richiede al candidato di dimostrare che ricopre il ruolo e possiede x anni di esperienza nel settore informatico:

Livello e-CF (media degli e-CF richiesti per il profilo)	Nr. minimo di anni di esperienza continuativa ricoprendo il ruolo per cui si candida (1 anno = 280 gg lavorativi equivalenti di lavoro)	Nr di anni di esperienza continuativa complessivi nel settore informatico/ICT/WEB (1 anno = 280 gg lavorativi equivalenti di lavoro)
5	3 *	4
4	2 *	4
3	2 *	2
2	1	2
1	6 mesi	1

* in caso di laurea magistrale specifica (ingegneria informatica o informatica), il numero minimo di anni di esperienza continuativa nel ruolo è ridotto di un anno (-1 rispetto a quanto riportato in tabella).

5.2.4 Riepilogo dei requisiti minimi

I requisiti minimi per l'accesso all'esame per il profilo di questo schema sono i seguenti:

Tipologia	**Requisito minimo**	**Alternativa equipollente al requisito minimo**
Formazione Formale: Titolo di studio	Laurea magistrale o master universitario di II livello	4 anni di esperienza nel settore informatico di cui 3 nella funzione
Formazione non formale Corsi specifici indicare durata ed eventuale qualifica o riconoscimento	8 crediti formativi conseguiti negli ultimi 12 mesi dalla presentazione della domanda	
Formazione in-formale (Anni di esperienza e Tipologia di esperienza)	4 anni di esperienza comprovata nella funzione	Riduzione a 2 anni di esperienza nel caso di possesso di titolo di studio di livello 5 EQF o superiore

L'analisi del curriculum viene eseguita con la verifica delle evidenze fornite dal candidato che ne attestano la formazione formale, non formale e informale.

6. PROCESSO DI CERTIFICAZIONE

6.1 Richiesta di ammissione all'esame

Sono ammessi a sostenere l'esame di certificazione tutti coloro che, dopo aver inoltrato richiesta attraverso il modulo Mod.04-MG, abbiano dimostrato il possesso dei requisiti richiesti dal presente schema.
Il modulo sopra citato, insieme al Tariffario, al Regolamento generale ed al Codice deontologico

sono disponibili sul sito https://certificazioni.istitutovolta.eu
La richiesta di certificazione contiene l'informativa sulla modalità di gestione dei dati personali attuata da Istituto Volta, secondo la documentazione reperibile sul sito.
Con la richiesta di certificazione il candidato si impegna a:

- mantenere riservate tutte le informazioni e i materiali ricevuti durante le prove d'esame;
- non divulgare notizie o informazioni inerenti le prove, lo svolgimento delle stesse, i documenti e le domande di cui viene a conoscenza durante l'esame.

In allegato alla richiesta di iscrizione, il candidato deve inviare i seguenti documenti:

- Curriculum vitae aggiornato, datato, firmato con richiamo agli articoli 46 e 76 del D.P.R. 445/2000 e alla legge sulla privacy;
- Copia di un documento d'identità in corso di validità;
- Evidenze dei requisiti di istruzione ed esperienza lavorativa per come richiesti ai paragrafi precedenti a supporto del CV;
- Copia della ricevuta di pagamento della quota relativa all'iscrizione all'esame (come da tariffario in vigore).

6.2 Analisi dei requisiti

Una volta ricevuti i documenti elencati al paragrafo precedente, Istituto Volta procederà all'analisi del soddisfacimento dei requisiti previsti, con particolare riguardo per l'analisi e la valutazione del CV.
Nel caso di incompletezze Istituto Volta segnalerà le integrazioni necessarie che il candidato dovrà fornire.
La richiesta sarà considerata accettata e comunicata al candidato nel momento in cui la documentazione sarà considerata completa ed adeguata rispetto ai requisiti e sarà stato effettuato il pagamento previsto dal tariffario in vigore.

6.3 Modalità di svolgimento dell'esame

Una volta fissata la data, Istituto Volta, almeno sette giorni prima della sessione d'esame, comunica per iscritto a tutti i candidati data, orari e luogo di svolgimento dell'esame. Tale comunicazione contiene anche i nomi degli esaminatori incaricati, allo scopo di consentire l'eventuale ricusazione motivata degli esaminatori incaricati, compresi i casi di conflitto di interesse che potrebbero emergere.
Analogamente, per garantire il rispetto del principio dell'imparzialità, agli esaminatori viene inviato, almeno dieci giorni prima della sessione d'esame, l'elenco dei candidati in modo da dare la possibilità di fornire la segnalazione di eventuali conflitti di interesse.
Alla sessione d'esame, oltre ai i candidati e alla commissione d'esame, possono essere presenti in qualità di osservatori:

- personale di Istituto Volta;
- personale dell'organismo di accreditamento;
- personale di altri organismi o enti di controllo.

6.3.1 Commissione di esame

La commissione d'esame deve essere composta da almeno un esaminatore per ogni 10 candidati presenti nella giornata d'esame.

Nel caso di più esaminatori la commissione nomina uno dei componenti come Presidente; qualora sia presente un unico esaminatore, questi riveste automaticamente il ruolo di Presidente.
Prima dell'inizio delle prove di esame i membri della commissione valutano ulteriormente situazioni di conflitto di interesse; qualora emergano circostanze di questo tipo dovrà essere fatta un'immediata segnalazione al Responsabile di schema di Istituto Volta. L'esame potrà essere svolto solo nel momento in cui i conflitti saranno stati risolti.
Gli esaminatori hanno l'obbligo di:

- verificare l'identità dei candidati rispetto alle domande di certificazione;
- mantenere la riservatezza sulle prove di esame;
- rispettare criteri di oggettività nella valutazione.

Gli esaminatori sono qualificati secondo quanto previsto dalla procedura PG.01 "Gestione degli esaminatori" nella versione valida.
La commissione d'esame, nel suo insieme, deve avere competenze superiori a quelle previste per i candidati che sostengono l'esame.

6.3.2 Identificazione dei candidati

Prima dell'inizio delle prove d'esame, i candidati sono tenuti a:

- esibire un documento di identità valido;
- firmare il registro di esame.

6.3.3 Regole comportamentali

Durante lo svolgimento delle prove d'esame, i candidati non possono consultare documenti, né usare telefoni cellulari, smartphone, tablet, né scambiare informazioni con altri candidati.
Il mancato rispetto di tali prescrizioni verrà valutato dal Presidente che potrà decidere di applicare sanzioni diverse, in base alla gravità dell'infrazione, fino all'interruzione dell'esame stesso.

6.3.4 Programma delle Prove

L'esame è costituito da 3 tipologie di prove eseguite nel seguente ordine:

1) Prova scritta con domande a risposta chiusa;
2) Prova scritta su scenari (simulazioni);
3) Prova orale.

Le prove si svolgeranno secondo lo schema di massima indicata nella tabella seguente.

ORARIO	ATTIVITA'
09:00	Identificazione dei candidati
09:30	Presentazione dell'esame, delle relative prove, della modulistica d'esame e della procedura relativa ai ricorsi e ai reclami
10:00	Prova scritta a risposte chiuse
11:00	Acquisizione degli esiti della prova scritta a risposte chiuse e avvio della relativa correzione. Preparazione della prova scritta su scenari.
11:30	Avvio della prova scritta su scenari.
13:00	Ritiro degli elaborati della prova scritta su scenari.
13.15	Pausa
14:15	Correzione della prova scritta su scenari.
15:30	Prove orali
18:00	Redazione del verbale finale

6.3.6 Descrizione delle prove e relativi criteri di valutazione

1) Prova scritta con domande a risposta chiusa

La prova scritta si compone di 20 domande che vertono sulle 5 aree dimensionali e-CF (**A. PLAN, B. BUILD, C. RUN, D. ENABLE, E. MANAGE**), tenendo conto delle aree e-competence e-CF specifiche della professione, inquadrate nei rispettivi livelli di difficoltà, descritti nel profilo alla voce 4 di questo schema.

Le domande sono a risposta chiusa con 4 alternative, di cui una sola esatta. La valutazione è fatta a fronte del modello delle risposte esatte.

Il candidato deve evidenziare la risposta per lui corretta, ciascuna risposta corretta vale 1 punto quelle sbagliate o non date valgono 0 punti; non vengono assegnati punteggi negativi.

Il candidato ha a disposizione **60 minuti** di tempo per svolgere la prova.
I criteri di valutazione sono i seguenti:

	Criterio	Esito
Esito Prova scritta	> 70 % risposte esatte (n. 14)	Prova superata
	> 60% e <70% risposte esatte (n.1	Necessità di ottenere una media finale > 70%
	<60 %	Prova non superata

2) Prova scritta su scenari (simulazione)
La seconda prova scritta consiste in uno scenario professionale che può vertere su interpretazioni, normativa applicabile, azioni da intraprendere.
Nella seconda prova si tiene conto come nella prima sia delle 5 aree dimensionali previste nella figura professionale che si certifica, sia delle competenze e-CF previste per tutti i profili e-CF degli aspetti trasversali di competenza relativi a: **Usabilità, Etica, Aspetti Legali ICT, Privacy, Sicurezza e sostenibilità**.
La correzione avviene durante la prova orale.
Il candidato ha a disposizione **1 ora e 30 minuti** di tempo per svolgere la prova.

3) Prova orale
La prova orale avrà inizio con la discussione della seconda prova scritta, in cui in candidato dovrà illustrare in modo dettagliato le azioni intraprese per raggiungere gli obiettivi dati.
Successivamente il commissario sottopone al candidato una serie di domande, indicativamente da 1 a 2, per verificare la competenza professionale dello stesso.
Il candidato ha a disposizione **20 minuti** di tempo per svolgere la prova.

Tutte le prove scritte e la prova orale, devono raggiungere il punteggio del 70% di risposte esatte. Per coloro che nella prima prova scritta sono tra il 60% e il 70% vale il requisito di media complessiva dei risultati delle prove almeno pari al 70%.
L'esame si considera superato quando la valutazione complessiva è superiore o uguale a 70/100, il candidato che ha totalizzato un punteggio inferiore non prosegue nell'iter di certificazione.

6.3.7 Verbale finale

Eseguite le valutazioni complessive la commissione redige il verbale, nel quale vengono riportate le informazioni salienti e dei risultati dell'esame. Nel verbale vengono riportati i candidati che hanno partecipato all'esame, con le relative valutazioni inerenti le prove sostenute da ciascuno di essi, fino a quella finale.
Nel verbale è previsto che siano riportati anche note sulla sede in cui è stato svolto l'esame.
Entro 5 giorni lavorativi dalla data dell'esame la commissione consegna il verbale al Comitato deliberante.

6.4 Delibera della certificazione

Il Comitato deliberante, dopo aver controllato l'analisi documentale, verificate le evidenze prodotte dal candidato e verificato il verbale finale di esame, delibera la certificazione se i requisiti di schema sono soddisfatti e l'esame di certificazione è positivo.

Successivamente Istituto Volta aggiorna il registro dei professionisti certificati per lo schema e lo pubblica sul sito https://certificazioni.istitutovolta.eu/ dandone successivamente comunicazione all'ente di accreditamento. La data di emissione del certificato, che determina l'inizio del periodo di validità, è quella corrispondente alla data nella quale viene eseguita la delibera da parte del comitato.

6.5 Certificato

Il certificato contiene le seguenti informazioni:
a. Riferimenti di Istituto Volta;
b. Nome, cognome della persona certificata e relativo codice fiscale;

c. Profilo di riferimento;
d. Numero identificativo del certificato;
e. Riferimento allo schema di certificazione;
f. Riferimento alla norma UNI 11506 nella versione in corso di validità;
g. Data di emissione della certificazione;
h. Data di ultima modifica e la data di scadenza del certificato.

La durata della certificazione è stabilità in 5 anni dalla data di delibera del certificato.
Il certificato è rilasciato sotto forma di tesserino.
Il certificato rimane di esclusiva proprietà di Istituto Volta, che ne concede l'utilizzo alla persona certificata per l'intero periodo di validità della certificazione.

7. USO DEL MARCHIO

Terminato positivamente l'iter di certificazione al professionista viene concesso l'uso del marchio di certificazione. Il professionista certificato si impegna ad accettare integralmente il presente regolamento come condizione per la concessione dell'uso del marchio di certificazione e del certificato stesso. Il mancato rispetto delle clausole del presente regolamento implica l'apertura di un'istruttoria di infrazione.

Per le modalità d'uso del marchio di Istituto Volta, si rimanda all'apposito Regolamento, pubblicato sul sito https://certificazioni.istitutovolta.eu/

8. MANTENIMENTO, RINNOVO, SOSPENSIONE, REVOCA E SUBENTRO DELLA CERTIFICAZIONE

8.1 Mantenimento

Le condizioni per il mantenimento annuale, per i quattro anni a seguito della certificazione, sono le seguenti:

- aver svolto la professione, da dimostrare tramite sottoscrizione di autodichiarazione rilasciata su apposito modello Mod.01-PG.07 "Richiesta di mantenimento/rinnovo";
- mancanza di reclami ricevuti dalle parti interessate o loro corretta gestione, da dimostrare tramite sottoscrizione di autodichiarazione rilasciata sul medesimo apposito modello Mod.01- PG.07;
- avere attivato processi di aggiornamento professionale per i crediti indicati in relazione al livello di qualifica e-CF riportato in tabella seguente (1 ora = 1 credito);
- avere effettuato il pagamento delle quote della prevista quota annuale.

Il Livello medio e-CF assegnato al professionista ottenuto con certificazione si deduce da quanto descritto al punto 4.

Livello medio e-CF assegnato	Nr crediti richiesti per anno (mantenimento)	Nr crediti richiesti totali (al rinnovo)
e-CF: da 4 a 5 (senior)	20	100
e-CF: da 2 a 3 (mid)	16	80
e-CF: 1 (junior)	8	40

8.2 Rinnovo

Entro tre mesi dalla data di scadenza, le persone certificate hanno l'obbligo di fornire la seguente documentazione:

- autodichiarazione rilasciata su apposito modello Mod.01-PG.07 "Richiesta di mantenimento/rinnovo" relativa all'assenza di reclami dalle parti interessate o alla loro

corretta gestione, se ricevuti;
- curriculum vitae aggiornato, da cui si ricava che è stata svolta la professione;
- avere attivato processi di aggiornamento professionale per i crediti indicati in relazione al livello di qualifica e-CF riportato nella tabella di cui al punto 8.1 (1 ora = 1 credito).

8.3 Sospensione

Nel caso in cui venga accertato che si è verificata anche una sola delle seguenti situazioni:
- violazione del codice deontologico;
- mancata richiesta di rinnovo entro il periodo previsto;
- mancato versamento della quota di iscrizione;
- mancata sottoscrizione, entro i termini previsti dal Regolamento generale, della documentazione contrattuale;
- mancata integrazione della documentazione richiesta al momento del rinnovo della certificazione;
- richiesta da parte della persona certificata;

viene applicato il provvedimento di sospensione.

8.4 Revoca

Nel in cui caso la persona certificata non provveda, entro i termini previsti, a risolvere le problematiche per cui è stato applicato il provvedimento di sospensione, OdC procede a ridurre il campo di applicazione o a revocare la certificazione.
La revoca comporta la cancellazione dal Registro delle persone certificate e viene comunicata all'eventuale Ente di Accreditamento.

8.5 Subentro

Qualora una persona già certificata come Security Specialist richieda a Istituto Volta di subentrare al precedente organismo, deve essere prodotta copia del certificato:
- se sotto accreditamento Istituto Volta provvederà a riemettere il certificato e al primo mantenimento procederà secondo quanto sopra previsto;
- se il subentro è da Ente non accreditato la persona non viene considerata certificata e deve intraprendere l'intero percorso di certificazione.

9. CODICE DEONTOLOGICO

Le persone certificate e/o in corso di certificazione si impegnano a rispettare il Codice Deontologico (CD)di Istituto Volta, pubblicato sul sito https://certificazioni.istitutovolta.eu/

10. REGOLAMENTO GENERALE

Le persone certificate e/o in corso di certificazione si impegnano a rispettare il Regolamento generale per la certificazione delle persone (RG) di Istituto Volta, pubblicato sul sito https://certificazioni.istitutovolta.eu/

11. RECLAMI E RICORSI

I candidati, i professionisti certificati o che non hanno ottenuto la certificazione, possono presentare *reclamo* contro l'operato degli organi di Istituto Volta, in merito alle decisioni prese nel processo di certificazione (es. ritardi nelle pratiche, comportamenti non corretti da parte degli esaminatori o di altro personale di Istituto Volta).
Istituto Volta provvede a registrare i reclami, analizzarli ed informare il reclamante in merito alle azioni intraprese, entro sessanta giorni dalla data di ricevimento del reclamo.
Qualora il reclamante non risulti soddisfatto della risposta ricevuta, o intenda opporsi ad una decisione di Istituto Volta può presentare *ricorso* per iscritto, motivando le ragioni del suo ricorso.
Per ricorso si intende la manifestazione esplicita e documentata di non accettazione delle decisioni adottate da Istituto Volta nell'ambito delle attività di certificazione del personale.
Istituto Volta fornirà al ricorrente risposta scritta e notificherà le eventuali azioni da intraprendere entro 60 giorni dalla data di ricevimento del ricorso.

Le modalità di dettaglio per la presentazione dei reclami e ricorsi sono riportate nel Regolamento generale per la certificazione delle persone (RG) di Istituto Volta, pubblicato sul sito https://certificazioni.istitutovolta.eu/