

**SCHEMA DI CERTIFICAZIONE: ISMSP (Accreditato Accredia)****Profilo professionale: PROFESSIONISTA DI SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI**

Il presente documento definisce i requisiti e le modalità per la certificazione delle competenze dei candidati per il profilo professionale della figura professionale ICT di cui alla norma UNI CEN EN ISO/IEC 27021 nel profilo di Information Security Management System Professional / professionista del sistema di gestione della sicurezza delle informazioni.

**IL VALORE AGGIUNTO DELLA CERTIFICAZIONE**

La norma ISO 27000 Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione richiama espressamente la ISO 27021 Tecnologie Informatiche – Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione – Requisiti come strumento per qualificare colui che gestisce i sistemi di gestione della sicurezza delle informazioni (semplificando, il responsabile della qualità della ISO 27001). Sino ad oggi l'unica certificazione possibile era quella del lead auditor ISO 27001 ma tale certificazione si basa su schemi proprietari autoreferenziali dato che non esiste una norma specifica per certificare il lead auditor (la ISO 27001 è una norma di certificazione di sistema non per le persone).

Il gruppo di lavoro ISO ha quindi riconosciuto la necessità di identificare in modo preciso e puntuale tale profilo, data la rilevanza che ricopre nel gestire i sistemi di sicurezza delle informazioni.

La ISO 27021 è basata sul syllabus dell'e-CF (European e-Competence Framework) ed ha molti punti di contatto con altre norme nazionali che utilizzano sempre l'e-CF, come la UNI 11506 e le declinazioni per i profili definiti nella UNI 11621-2 e parte UNI 11621-3 soprattutto nelle figure dell'ICT security manager, ICT security specialist e WEB security expert. La norma ha anche molti punti di contatto con la norma UNI 11697 relativa al DPO e auditor privacy proprio perché la base di riferimento la l'e-CF.

La certificazione del profilo del professionista dei sistemi di gestione della sicurezza delle informazioni effettuata da Intertek avviene sotto accreditamento Accredia ISO 17024 in accordo alla Legge 4/2013 Disposizioni in materia di professioni non organizzate.

**REQUISITO DI LEGGE**

Non vi è quadro legislativo di riferimento trattandosi di professione libera ai sensi della Legge 4:2013.

**REQUISITI PER ACCEDERE ALLA CERTIFICAZIONE**

Ai fini dell'accesso al processo di valutazione di conformità (esame di certificazione), si riportano di seguito i seguenti requisiti:

Apprendimento formale	Laurea. In alternativa 4 anni di esperienza nel settore informatico di cui 3 nella funzione. In caso di laurea afferente al settore informatico, 3 anni di esperienza ma solo 2 nella funzione.
Apprendimento non formale	Non è richiesto un corso specifico di accesso.
Apprendimento informale	Ricoprire il ruolo e avere 3 anni di esperienza nel settore informatico di cui 2 nella funzione. In caso di laurea afferente al settore informatico, 3 anni di esperienza ma solo 2 nella funzione.

Per richiedere di partecipare ad un esame è necessario inoltrare, oltre quanto sopra:

- ① Domanda di certificazione
- ① Documenti di identità
- ① Liberatoria privacy generale o per esami online



- ④ Curriculum vitae, datato, firmato con consenso al GDPR e ai sensi degli artt. 46 e 76 del Dlgs 445/2000
- ④ Evidenze della formazione e degli anni di esperienza nello specifico ruolo
- ④

**DURATA DELLA CERTIFICAZIONE - REQUISITI DI MANTENIMENTO E RINNOVO**

La durata della certificazione è pari a cinque anni.

I requisiti di mantenimento annuale e rinnovo quinquennale sono:

Assenza di reclami	Dichiarazione ai sensi della legge 4:2013.
Apprendimento non formale	Avere attivato processi di aggiornamento professionale per 8 crediti.
Continuo esercizio della professione	Continuità nell'esercizio della professione.

**VALIDITA' DELLA CERTIFICAZIONE – SOSPENSIONE E REVOCA**

La validità dei certificati è subordinata al soddisfacimento dei requisiti di mantenimento annuale. In caso in cui la persona certificata non dovesse fornire le evidenze dovute in fase di mantenimento (onere in capo alla persona certificata), Intertek provvederà alla sospensione del certificato trascorsi trenta giorni dalla data di mantenimento prevista. La sospensione avrà durata massima pari a dodici mesi dalla data di mantenimento, fatto salvo diverso requisito espresso dalla norma specifica. Trascorsi i dodici mesi, il certificato verrà revocato.

**ESAME DI CERTIFICAZIONE**

L'Esame è condotto sulle conoscenze ed abilità definite nella normativa di riferimento da esaminatori qualificati. Si applica il principio della peer certification (ISO 17040) ovvero gli esaminatori sono dei pari, rispetto ai candidati, ma qualificati per condurre esami.

Le prove si svolgeranno nel seguente ordine e vengono somministrate separatamente:

- Prova scritta 1 (30 domande a risposta chiusa, tempo a disposizione 45 minuti)
- Prova scritta 2 (Prova scritta 5 domande scenario, tempo a disposizione 45 minuti)
- Prova orale ( 20 minuti)

Le prove non possono essere invertite. Per accedere all'esame orale il candidato deve aver ottenuto almeno un punteggio del 60% di risposte corrette nella prova scritta.

L'esame può essere condotto anche in modalità online. Al termine della valutazione complessiva del candidato la commissione d'esame lo informa dell'esito dell'esame ricordando che, se positivo, la delibera finale spetta al comitato di delibera.

**COSTO DELLA CERTIFICAZIONE**

Il costo della certificazione è di € 600 + IVA.

Si precisa che le tariffe possono usufruire di scontistiche sulla base di convenzioni specifiche.

Alle persone certificate viene fornito un certificato in formato digitale.



## SERVIZI AGGIUNTIVI

- ④ Certificato in inglese
- ④ Tesserino
- ④ Timbro
- ④ Open badge

