AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

e-CF*plus*

SCHEMA DI CERTIFICAZIONE DEL PROFILO

ICT Security Manager

Requisiti minimi	**ICT Security Manager**
Esperienza di lavoro nel profilo	36 mesi
Competenze esercitate	**Sviluppo della Strategia della Qualità ICT – ICT Quality Strategy Development** Definisce, migliora e perfeziona una strategia formale per soddisfare le aspettative e migliorare le performance del business cliente (bilanciamento tra costi e rischi). Identifica i processi critici che influenzano la service delivery e le performance del prodotto per definirli nel sistema di gestione della qualità ICT (rif D.4). Usa gli standard definiti per formulare gli obiettivi di qualità della gestione del servizio, del prodotto e del processo. Identifica le responsabilità di gestione della qualità ICT. Esercita la leadership strategica nel radicare la qualità ICT (es. metriche e miglioramento continuo) nella cultura dell'organizzazione. Esempi di conoscenza (k) e abilità (s): K1 i principali framework dell'industria dell'information technology - COBIT, ITIL, CMMI, ISO – e le loro implicazioni per la governance dell'ICT aziendale K2 la strategia aziendale dell'informazione K3 i differenti modelli di servizio(SaaS, PaaS, IaaS) e operativi (es. Cloud Computing) S1 definire una politica di qualità dell'ICT per soddisfare gli standard di performance dell'organizzazione e gli obiettivi della customer satisfaction S2 identificare le metriche di qualità da utilizzare S3 applicare standard e best practice utili per mantenere la qualità dell'informazione **Gestione del Rischio – Risk Management** Implementa la gestione del rischio dei sistemi informativi attraverso l'applicazione delle politiche e procedure definite dall'azienda per il risk management. Valuta il rischio per il business dell'organizzazione e documenta rischi potenziali e piani di prevenzione. 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 audit sui processi ICT e sull'ambiente. Esempi di conoscenza (k) e abilità (s): 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 best practice (metodologie) e gli standard nella analisi del rischio S1 sviluppare piani di risk management 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 dell'emergenza **Governance dei Sistemi Informativi – IS 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. Fornisce la leadership per la governance della strategia dei sistemi informativi comunicando, diffondendo e controllando i principali processi in tutta la infrastruttura ICT. Esempi di conoscenza (k) e abilità (s) K1 l'infrastruttura ICT e l'organizzazione del business K2 la strategia di business dell'azienda K3 i valori del business 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 key performance indicators (KPI's) S4 comunicare il valore, i rischi e le opportunità derivanti dalla strategia del sistema informativo **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 applicare strategia e policy specifiche per un miglioramento continuo della sicurezza fornita. Fornisce la leadership per l'integrità, la riservatezza e la disponibilità dei dati presenti nei sistemi informativi e assicura la conformità con i requisiti legali Esempi di conoscenza (k) e abilità (s) 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'auditing interno del sistema informativo K5 le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale K6 le tecniche di attacco informatico e le contromisure per evitarli K7 la computer forensics 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 auditing di sicurezza S5 applicare tecniche di monitoraggio e collaudo S6 stabilire un piano di ripristino S7 implementare il piano di ripristino in caso di crisi
Esempio di deliverable documentabile	Strategia Sicurezza delle informazioni e Politica di gestione dei rischi oppure Politica Sicurezza delle informazioni
Esami scritti con valutazione automatica	Eucip Core Plan