



REGIONE AUTONOMA DE SARDIGNA  
REGIONE AUTONOMA DELLA SARDEGNA

#### Area di attività

Codice AdA	9999433
Denominazione AdA	Gestione della sicurezza dell'informazione ai sensi del GDPR
Descrizione della performance	Implementare la politica della sicurezza dell'informazione. Controllare e prendere iniziative a fronte di intrusioni, frodi e buchi o falle della sicurezza. Assicurare che i rischi legati alla sicurezza siano analizzati e gestiti per i dati e le informazioni aziendali. Rivedere gli incidenti sulla sicurezza e fornire raccomandazioni per applicare strategia e policy specifiche. Garantire il rispetto degli adempimenti previsti dalle leggi vigenti, con particolare riferimento alle norme in materia di privacy e sicurezza informatica, per minimizzare i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme ai sensi del Regolamento (UE) 2016/679 e s.m.i.
Osservabilità	Per quanto concerne il primo criterio per la riflessione in merito alle tipologia di prova applicabili, si rileva che la prestazione può essere realizzata in condizioni controllate dal punto di vista spaziale, temporale e tecnologico, ma implica un contatto diretto con interlocutori interni (alti livelli decisionali): essa dunque non risponde completamente al criterio di osservabilità.
Tipologia di performance	Per quanto riguarda la tipologia di performance, nella UC prevale una dimensione di processo: la valutazione si basa infatti sulla più o meno corretta gestione della sicurezza dell'informazione e delle scelte organizzative. La prova più adeguata risulta essere il Project work, poiché consente di far emergere i processi logici e i le tecniche che sottostanno alla pianificazione delle strategie ritenute più adeguate. Al fine di valutare le interazioni con i massimi livelli decisionali può essere utile prevedere un colloquio come integrazione.
Visibilità	Per quanto concerne infine il terzo criterio (visibilità), la prestazione risulta scarsamente visibile: sarà necessario dunque prevedere una integrazione (ad es. attraverso un colloquio, o specifiche prove oggettive di conoscenza) per esplicitare sia le componenti di carattere decisionale della performance, che alcune specialistiche.
Tipologia di prova preferibile	Project-work
Tipologia di prova integrativa	Colloquio
Tipologia di prova adatta	-

#### Unità di competenza

Codice unità di competenza	1048
Livello EQF	6
Abilità	



REGIONE AUTONOMA DE SARDIGNA  
REGIONE AUTONOMA DELLA SARDEGNA

	<ol style="list-style-type: none"><li>1. Adeguare i sistemi alla normativa vigente</li><li>2. Analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi</li><li>3. Costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi</li><li>4. Definire dei piani di formazione/informazione al personale e a soggetti esterni sui sistemi di sicurezza</li><li>5. Definire gli standard di sicurezza</li><li>6. Definire procedure tecniche conformi alle normative vigenti per consentire l'accesso ai dati da parte del titolare o del responsabile del trattamento anche in assenza degli incaricati</li><li>7. Definire un piano di formazione ed addestramento in materia di sicurezza informatica e di privacy per gli incaricati del trattamento dei dati personali, gli amministratori e gli utenti del sistema informativo</li><li>8. Documentare la politica di gestione della sicurezza collegandola alla strategia di business</li><li>9. Effettuare auditing di sicurezza</li><li>10. Minimizzare i rischi di distruzione o perdita (anche accidentale) dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme ai sensi della vigente normativa su privacy e tutela dei dati, secondo quanto stabilito dal Regolamento (UE) 2016/679 e ss.mm.ii.</li></ol>
Conoscenze	<ol style="list-style-type: none"><li>1. I rischi critici per la gestione della sicurezza</li><li>2. La computer forensics</li><li>3. La normativa vigente e i trattati internazionali sulla protezione dei dati, in particolare normative vigenti in materia di privacy e tutela dei dati personali (Regolamento (UE) 2016/679 e ss.mm.ii.) per assicurare il costante rispetto delle disposizioni di legge</li><li>4. La politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti e le tipologie di dati personali comuni e sensibili per valutare correttamente gli obblighi previsti dalla normativa in relazione alla tipologia di dati presenti nelle varie aree del sistema informativo</li><li>5. L'approccio all'auditing interno del sistema informativo</li><li>6. Le best practice e gli standard nella gestione della sicurezza delle informazioni</li><li>7. Le tecniche di attacco informatico e le contromisure per evitarli</li><li>8. Le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale</li><li>9. Misure di sicurezza obbligatorie previste dalle vigenti normative in materia di privacy, tutela dei dati personali e sicurezza informatica, per assicurare il rispetto della legge e ridurre i rischi di sanzioni penali ed amministrative</li><li>10. Responsabilità civili e penali connesse alla violazione della sicurezza informatica per valutare concretamente i rischi di sanzioni penali o amministrative legate alla gestione del sistema informativo</li></ol>

#### Standard Formativi

Documento Standard Formativi	
Note	



REGIONE AUTÓNOMA DE SARDIGNA  
REGIONE AUTONOMA DELLA SARDEGNA

Data e ora ultimo caricamento	
-------------------------------	--

#### Profili di Qualificazione associati