“Exploring the AI Frontier: AI-Driven Cyber Risk Management for SMEs”

KA210-VET

Mappa delle competenze

Introduzione

La Mappa delle competenze AID è un quadro strutturato progettato per identificare e classificare le competenze critiche necessarie alle PMI per affrontare efficacemente la trasformazione digitale e gestire i rischi legati all'intelligenza artificiale. Allineata ai livelli del Quadro europeo delle qualifiche (EQF), la mappa garantisce che la preparazione digitale e la resilienza siano misurabili e standardizzate nei diversi contesti europei. La struttura della mappa è organizzata in tre aree prioritarie: sicurezza informatica, gestione dei rischi informatici e analisi dei dati. Per ciascuna area, il quadro fornisce una suddivisione completa in comportamenti, competenze, conoscenze e attitudini.

- **Comportamenti**: Descrivono azioni osservabili e processi decisionali, come l'applicazione di politiche strutturate di gestione dei rischi, l'identificazione dei pregiudizi (*bias*) algoritmici e l'uso responsabile dei dati personali.
- **Abilità**: Questa dimensione si concentra sull'applicazione pratica, compresa la configurazione delle impostazioni di sicurezza, l'identificazione e la priorizzazione delle minacce informatiche, nonché la raccolta e la pulizia dei dati provenienti da diverse fonti.
- **Conoscenze**: Rappresentano le basi teoriche necessarie, come la comprensione dei concetti fondamentali di cybersecurity, la conoscenza dei vettori di attacco più diffusi, degli standard di gestione del rischio e dei principi etici dell'IA.
- **Responsabilità /Autonomia**: Evidenziano la forma mentis essenziale, tra cui la proattività nella prevenzione dei rischi, una mentalità analitica per decisioni basate sui dati e l'impegno costante nel garantire l'integrità delle informazioni.

Per avere una panoramica del processo di creazione della mappa delle competenze, si possibile consultare lo studio sulle competenze per la resilienza digitale e la crescita delle piccole e medie imprese *Competency Research for Digital Adaptation and Growth in SMEs* (Deliverable 1) e il report sull’indagine sul divario delle competenze digitali delle PMI *International Report on SME Digital Competence Gap Survey Results* (Deliverable 2) condotti nei paesi

Finanziato dall’Unione europea. Le opinioni espresse appartengono tuttavia al solo o ai soli autori e non riflettono necessariamente le opinioni dell’Unione europea o dell’Agenzia Nazionale per lo Sviluppo dell’Istruzione (VIAA). Né l’Unione europea né l’autorità concedente (VIAA) possono esserne ritenute responsabili.

partner: Italia, Lettonia e Turchia. I documenti sono disponibili in inglese sul sito web del progetto: https://www.bda.lv/en/ai-driven-cyber-risk-management-for-smes/

Finanziato dall'Unione europea. Le opinioni espresse appartengono tuttavia al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia Nazionale per lo Sviluppo dell'Istruzione (VIAA). Né l'Unione europea né l'autorità concedente (VIAA) possono esserne ritenute responsabili.

Area di competenze e descrizione	Comportamenti	Abilità	Conoscenze	Responsabilità/autonomia
Competenze di sicurezza informatica **La capacità di proteggere i dispositivi digitali, i sistemi, i dati aziendali e le attività personali online da minacce e rischi. Questo avviene applicando pratiche sicure, rispettando la privacy e prendendo decisioni informate sull'uso delle tecnologie esistenti ed emergenti (inclusa l'intelligenza artificiale), per garantire un ambiente digitale sicuro e affidabile.**	1. Proteggere i dispositivi e i contenuti aziendali da minacce e rischi digitali. 2. Conoscere le pratiche di base di cybersecurity e privacy per favorire la fiducia negli strumenti digitali. 3. Garantire il rispetto dei dati personali e della privacy negli ambienti digitali. 4. Utilizzare e condividere i dati personali in modo responsabile. 5. Comprendere le informative sulla privacy e le loro implicazioni. 6. Evitare stress, affaticamento o altri rischi per la salute legati all'uso del digitale. 7. Riconoscere e prevenire comportamenti online dannosi (es. cyberbullismo).	1. Identificazione e risposta ai rischi di sicurezza per dispositivi e dati. 2. Configurazione delle impostazioni di sicurezza dei dispositivi. 3. Utilizzo dell'autenticazione a più fattori (MFA) e di password sicure. 4. Archiviazione sicura e backup dei dati. 5. Valutazione della credibilità e dell'affidabilità degli strumenti di IA.	1. Conoscere i concetti fondamentali di cybersecurity (autenticazione, crittografia, backup dei dati). 2. Conoscere i cyber-attacchi più comuni (malware, phishing, ransomware, ecc.). 3. Applicare pratiche digitali sicure per uso lavorativo e personale. 4. Essere consapevoli di leggi e normative comuni che regolano i dati digitali (GDPR, leggi nazionali, ecc.). 5. Conoscere i principi base del machine learning e uso sicuro dell'IA.	1. Proattività verso la cybersecurity e la prevenzione dei rischi. 2. Gestire in modo responsabile dei dati aziendali e personali. 3. Flessibilità e apertura all'apprendimento di nuove tecnologie. 4. Giudizio critico verso le comunicazioni e l'uso di strumenti e ambienti digitali.

Finanziato dall'Unione europea. Le opinioni espresse appartengono tuttavia al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia Nazionale per lo Sviluppo dell'Istruzione (VIAA). Né l'Unione europea né l'autorità concedente (VIAA) possono esserne ritenute responsabili.

Area di competenze e descrizione	Comportamenti	Abilità	Conoscenze	Responsabilità/autonomia
	8. Promuovere l'inclusione digitale e il benessere sociale attraverso la tecnologia. 9. Comprendere i bias (pregiudizi) algoritmici e la spiegabilità nei sistemi di IA. 10. Valutare l'affidabilità e l'efficacia degli strumenti di cybersecurity basati sull'IA. 11. Prendere decisioni informate sull'adozione dell'IA per il rilevamento delle minacce.		6. Conoscere gli aspetti etici e legali dell'uso dell'IA.	

Area di competenze e descrizione	Comportamenti	Abilità	Conoscenze	Responsabilità/autonomia
Gestione del rischio informatico **La capacità di identificare, analizzare e dare priorità ai rischi per gli asset digitali, i sistemi informativi e i dati. Comporta il prendere decisioni informate e allineate al business che bilancino sicurezza, costi e necessità operative, al fine di proteggere se stessi e l'organizzazione e supportare gli obiettivi strategici.**	1. Applicare politiche strutturate di gestione del rischio in tutti i sistemi IT. 2. Valutare i rischi per gli asset digitali e pianificare strategie appropriate. 3. Presentare analisi costi-benefici per supportare le decisioni sui rischi informatici. 4. Allineare le decisioni di gestione del rischio con gli obiettivi aziendali e tecnologici. 5. Valutare la cybersecurity posture e definire obiettivi specifici per l'azienda 6. Identificare rischi, costi e punti deboli durante la	1. Identificare, classificare e dare priorità ai rischi informatici. 2. Eseguire valutazioni del rischio qualitative e quantitative. 3. Comunicare in modo efficace i rischi tecnici in approfondimenti rilevanti per le aziende 4. Creare strategie di mitigazione del rischio e piani d'azione realistici. 5. Comunicare i rischi informatici e le relative strategie agli stakeholder tecnici e non.	1. Conoscere i framework di gestione del rischio e degli standard di qualità pertinenti. 2. Conoscere il panorama della sicurezza informatica e dei rischi per le aziende 3. Essere consapevole dell'importanza di analizzare, comunicare e rispondere agli incidenti di sicurezza informatica. 4. Conoscere	1. Giudizio equilibrato tra sicurezza, costi e usabilità. 2. Responsabilità nella protezione del valore aziendale, non solo della tecnologia. 3. Mentalità analitica, presa di decisioni basate sui fatti 4. Collaborazione tra reparti di sicurezza, IT e business. 5. Approccio lungimirante nell'anticipare i rischi emergenti.

Finanziato dall'Unione europea. Le opinioni espresse appartengono tuttavia al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia Nazionale per lo Sviluppo dell'Istruzione (VIAA). Né l'Unione europea né l'autorità concedente (VIAA) possono esserne ritenute responsabili.

	pianificazione delle azioni di sicurezza informatica 7. Gestire i rischi relativi ai dati aziendali e ai patrimoni informativi.		modelli decisionali basati sul rischio e sull'analisi costi-benefici. 5. Essere consapevoli dei requisiti normativi, legali e di conformità (compliance) per dati e sistemi all'interno delle aziende.	

Finanziato dall'Unione europea. Le opinioni espresse appartengono tuttavia al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia Nazionale per lo Sviluppo dell'Istruzione (VIAA). Né l'Unione europea né l'autorità concedente (VIAA) possono esserne ritenute responsabili.

Area di competenze e descrizione	Comportamenti	Abilità	Conoscenze	Responsabilità/autonomia
Gestione e analisi dei dati **La capacità di raccogliere, elaborare, interpretare e comunicare dati applicando metodi analitici, proteggendo l'integrità e la privacy dei dati e trasformando informazioni complesse in conoscenza significativa e operativa che supporti processi decisionali informati**	1. Comprendere come i dati personali vengono elaborati e protetti. 2. Applicare analisi costi-benefici e valutazione del rischio in contesti legati ai dati 3. Raccogliere e preparare dati di qualità provenienti da diverse fonti 4. Utilizzare metodi statistici per comprendere i dati ed estrarre approfondimenti (insight). 5. Presentare i dati visivamente per garantire una comunicazione e decisioni chiare.	1. Raccogliere, pulire e strutturare dati da varie fonti. 2. Utilizzare tecniche statistiche e analitiche per l'analisi dei dati. 3. Visualizzare dati a supporto del processo decisionale aziendale (tabelle, grafici, presentazioni, ecc.). 4. Trarre conclusioni e prendere decisioni basate sui dati. 5. Identificare tendenze e correlazioni nei dati utilizzando il pensiero critico.	1. Conoscere il ciclo di vita, la garanzia della qualità e i principi di gestione dei dati. 2. Conoscere metodi statistici e analitici per l'elaborazione dei dati. 3. Privacy ed etica nell'uso dei dati personali (GDPR, anonimizzazione dei dati). 4. Conoscere strumenti e tecniche di data visualization. 5. Conoscsre modelli di analisi costi-benefici e del rischio per	1. Capacità e volontà di esplorare i dati e mettere in discussione i presupposti esistenti. 2. Impegno nel mantenere l'accuratezza e l'integrità dei dati. 3. Obiettività dell'analisi e uso dei dati in contrapposizione all'intuizione. 4. Responsabilità nella comunicazione e nell'interpretazione dei dati.

Finanziato dall'Unione europea. Le opinioni espresse appartengono tuttavia al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia Nazionale per lo Sviluppo dell'Istruzione (VIAA). Né l'Unione europea né l'autorità concedente (VIAA) possono esserne ritenute responsabili.

	6. Spiegare i risultati di analisi complesse in modo chiaro e orientato all'azione. 7. Porre domande critiche e identificare schemi (pattern) di dati nascosti. 8. Aggiornare continuamente le proprie competenze con nuovi strumenti, metodi e best practice.		decisioni basate sui dati.	

Finanziato dall'Unione europea. Le opinioni espresse appartengono tuttavia al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia Nazionale per lo Sviluppo dell'Istruzione (VIAA). Né l'Unione europea né l'autorità concedente (VIAA) possono esserne ritenute responsabili.