PIANO DI FORMAZIONE NAZIONALE IN MATERIA DI *CYBER SECURITY, CYBER THREAT, PRIVACY*

ALLEGATO 2 – CATALOGO FORMATIVO

Livello Awareness: Selezione Esemplificativa Corsi Base

Corso		Obiettivo	Durata (hh)
1	Cybersecurity Awareness generale	Focus sulla sicurezza individuale, Aspetti comportamentali, normativi, Codici dell'Amministrazione Digitale, Aspetti Tecnologici di base	8
2	Privacy & Data Protection awareness	Aspetti normativi, ruoli, responsabilità e misure rilevanti, Privacy Impact Analysis, Risk Management, Privacy by Design e by Default	8
3	Corso di formazione di base in Cybersecurity per funzionari PA Task Force sicurezza informatica – Fase 1	Conoscere quali tipi di attacchi può subire un dispositivo di elaborazione dati e saper utilizzare tecniche, comportamenti e programmi per difendere il patrimonio fisico e quello informativo	20
4	Corso di formazione di base in Cybersecurity per funzionari pa task force sicurezza informatica – Fase2: Follow Up Laboratoriale– Livello Awareness	Esempi di casi reali di attacchi informatici con valutazione di soluzioni operative; Utilizzo di carte e di token fisici per accessi con maggiore livello di protezione; Impostazioni personalizzate dei programmi di difesa; Programmi per il recupero di dati cancellati Programmi di sincronizzazione dati per il salvataggio delle basi di dati; Indicazione di tecniche di salvataggio dei file modificati, in tempo reale e in tempo differito	20
5	Advanced Persistent Threats Awareness	Tipologie di vulnerabilità umane e tecnologiche, Principali tipologie di attacco, modalità di attacco a Sistemi e Informazioni	8
6	Laboratorio Pratico di ICT & Cyber Security	Laboratorio pratico di simulazione scenari d'attacco e tecniche e strumenti di prevenzione, mitigazione e recovery, approfonditi nelle implicazioni organizzative e di Business secondo le norme ISO 27001, 22301 e 20000.1.	24
7	Certificazione base CSX Cybersecurity Fundamentals di ISACA Certificazione	L'esame CSX Cybersecurity Fundamentals di ISACA è il primo livello di certificazione internazionale delle competenze organizzative, tecniche, ed operative in materia di CyberSecurity secondo il Framework del NIST	16
8	Certificazione base COBIT for NIST per le Misure di Controllo Certificazione	Il corso ha l'obiettivo di approfondire gli obiettivi del Cybersecurity Framework (CSF) NIST ed i suoi sette step implementativi relativi a processi e misure di controllo secondo il modello COBIT5.	24
9	Tecniche e strumenti di IT Risk Analysis – Livello Awareness	Il corso approfondisce i processi di Information Security Management System, fornendo linee guida e metodologia per la mappatura di ruoli, responsabilità, attività e processi e per l'identificazione dei processi critici dell'organizzazione, con approfondimento particolare sulla Business Impact Analysis.	8
10	Tecniche e strumenti di Business Continuity, Disaster Recovery ed Incident Management – Livello Awareness	Il corso fornisce la metodologia e le linee guida per progettare e realizzare la soluzione, che comprende la strategia e il piano per la continuità operativa dell'organizzazione e il piano per la gestione dell'emergenza e il ripristino delle attività ICT a seguito di disastro.	8