CORSO CYBERSECURITY
COME NAVIGARE IN MANIERA SICURA

Corso Cybersecurity per la "Formazione del personale scolastico per la transizione digitale (D.M. 66/2023)"

Sono state pubblicate le Istruzioni operative (prot. n. 141549 del 7 dicembre 2023) che forniscono indicazioni alle scuole beneficiarie, individuate quali nodi formativi locali del sistema di formazione per la transizione digitale, per la progettazione e la gestione degli interventi nell'ambito dell'investimento 2.1 "**Didattica digitale integrata e formazione alla transizione digitale per il personale scolastico**" della Missione 4 – Componente 1 del PNRR.

Gli interventi sono finalizzati alla realizzazione di percorsi formativi per il personale scolastico (dirigenti scolastici, direttori dei servizi generali e amministrativi, personale ATA, docenti, personale educativo) sulla transizione digitale nella didattica e nell'organizzazione scolastica, in coerenza con i quadri di riferimento europei per le competenze digitali DigComp 2.2. e DigCompEdu.

Il nostro corso Cybersecurity è adattabile alla Linea di investimento 2.1 "*Didattica digitale integrata e formazione alla transizione digitale per il personale scolastico*"

Finalità del percorso

Acquisire conoscenze utili a sviluppare investimenti in innovazione, digitalizzazione dei processi produttivi, economia circolare, sviluppo equo e sostenibile, green economy e cybersecurity.

Contenuti del percorso

Il corso proposto nasce dall'esigenza di rispondere in modo sempre più strutturato alla necessità di protezione e governo della sicurezza informatica, pertanto approfondisce gli aspetti tecnici, legali, gestionali legati alla sicurezza e alla privacy. Si registrano oramai quotidianamente attacchi di varia natura e con finalità diverse fra cui il furto di dati personali, dati critici per le organizzazioni e blocco delle operazioni. Ormai tutto è digitale e connesso e la sicurezza informatica è diventato un elemento strategico fondamentale. Le soluzioni informatiche per la sicurezza non possono essere trascurate pena il blocco del funzionamento dei processi aziendali. La cyber security va gestita con strategie proattive attraverso il cyber risk assessment per anticipare il potenziale rischio e con strategie reattive attraverso il cyber emergency response plan per affrontare l'eventuale incidente. Occorre quindi impostare dei piani che tengano conto delle minacce e di tutti i rischi prima che essi si verifichino. Ogni realtà vive dei propri dati ed in questi è concentrato un elevato valore. La sicurezza dei servizi web è fortemente legata al rapido aumento delle connessioni e degli utenti, all'aumento del valore delle transazioni, alla crescita del commercio elettronico. La sicurezza delle informazioni è pertanto un elemento integrante della strategia di trasformazione digitale ed è fondamentale comprendere i principali driver e le soluzioni. Dotarsi di adeguati protocolli di cyber security può essere determinante. La security è fatta di processi e procedure, soprattutto nella digital transformation e va pertanto integrata nel business workflow delle pubbliche amministrazioni. Si parla, infatti, di "digital journey" e deve essere su misura di tutte le pubbliche amministrazioni per diventare davvero efficace anche nelle complessità dei nuovi ambienti digitali. Per questo è molto importante avere un sistema di monitoraggio di quello che accade nelle proprie reti e infrastrutture digitali. Molti degli attacchi arrivano, dall'interno, da errori umani e per questo bisogna considerare il rischio nel momento stesso in cui si progetta la digital transformation. La sicurezza informatica è diventata il motore abilitante che consente di accelerare il loro passaggio al cloud e di sfruttare la velocità, la scalabilità e la resilienza della trasformazione digitale e rappresenta un fattore di differenziazione, diventando così il motore abilitante che consente di accelerare e di sfruttare la velocità, la scalabilità e la resilienza della trasformazione digitale. Il corso ha quindi lo scopo di trasferire conoscenze sulla Cybersecurity, quale kit di misure organizzative, tecnologiche e di processo fondamentale per sviluppare specifiche capacità per proteggere le informazioni da attacchi che possono provocarne la perdita, la diffusione incontrollata, la compromissione o la mancata disponibilità, creando un danno concreto al business e all'immagine: conoscenze, metodologie, strumenti, normative ed abilità per sviluppare per gestire e monitorare in maniera efficace ed efficiente i propri sistemi informativi, al fine cogliere le opportunità offerte dalla digital transformation.

Articolazione didattica (6 ore)

UF_1 STRATEGIA & PREREQUISITI 2 ore: fondamenti di cybersecurity ed impostazione strategica, sicurezza collaborativa ed il lavoro di squadra.

UF_2 GDPR ED AVVIO DEL PIANO CYBERSECURITY 2 ore: GDPR ed il trattamento dei dati, come iniziare un piano per affrontare la cybersecurity, partendo dall'esistente.

UF_3 LA TIPOLOGIA DEGLI ATTACCHI E MECCANISMI DI DIFESA 2 ore: ransomware, spyware, whaling, phishing, data breach, gli attacchi più diffusi settorialmente. Antivirus, Firewall, aggiornamenti, VPN.

Cordiali saluti.

Contatti:
dcaformazione@gmail.com
+39 320 70 69 678
Dott. Antonio Basile
www.dcaformazione.it