

CORSO FAD AWARENESS NIS 2 PER LO STAFF

Obiettivo: sviluppare comportamenti sicuri (cyber hygiene), la capacità di riconoscere minacce (in particolare il phishing) e l'adesione alle procedure di segnalazione di incidenti/eventi sospetti.

SOGGETTI DESTINATARI	OBIETTIVI	CONTENUTI
Medici, Infermieri, Tecnici sanitari, Amministrativi	• Apprendere le pratiche di “basic cyber hygiene” richieste dalla NIS2 e dalle linee guida ENISA (password sicure, riconoscimento phishing, comportamento sicuro). • Riconoscere segnali di phishing, ransomware e compromissione account. • Saper eseguire correttamente la segnalazione interna di incidenti o eventi sospetti. • Comprendere la criticità dei dati sanitari e la loro gestione responsabile.	• Introduzione alla NIS2 e al rischio Cyber. • Minacce più comuni nel settore sanitario (phishing, ransomware, compromissioni e-mail). • Riconoscere e-mail sospette e comportamenti pericolosi. • Uso sicuro dei dispositivi IT (clinici e non) e delle credenziali. • Protezione dei dati del paziente e del fascicolo sanitario elettronico. • Procedure di segnalazione incidenti o anomalie.

ARTICOLAZIONE DEL CORSO

MODULO	DURATA	CONTENUTI CHIAVE
A1 – Introduzione NIS2	20'	Perché la cybersicurezza è sicurezza del paziente; responsabilità individuali; principi base; canali di supporto e segnalazione.
A2 – Cyber hygiene in pratica	30'	Credenziali e MFA; workstation locking; aggiornamenti; gestione dispositivi mobili; uso sicuro di USB e supporti rimovibili; lavoro da remoto.
A3 – Phishing, social engineering e frodi	30'	Indicatori; casi tipici; email/sms/telefonate; verifiche a due vie; cosa fare e cosa non fare.
A4 – Gestione sicura dei dati e strumenti collaborativi	20'	Classificazione e condivisione; dati sanitari; invii e allegati; cloud e strumenti aziendali; stampa e smaltimento documenti.
A5 – Segnalazione incidenti e near miss	20'	Quando segnalare; quali informazioni fornire; escalation; importanza della tempestività; no blame culture.
TOT	120'	

STRUMENTO DI VERIFICA DELL'APPRENDIMENTO

Test di apprendimento a risposta multipla