Cybersecurity e Data protection: dalla normativa alle applicazioni pratiche

Obiettivo formativo:

Applicazione nella pratica quotidiana dei principi e delle procedure dell'evidence-based practice (EBM – EBN – EBP)

Numero crediti formativi:

4,5 crediti ECM

Professioni mediche accreditate:

Medico chirurgo , Farmacista, Psicologo, Biologo, Chimico, Fisico, Assistente sanitario, Dietista, Fisioterapista, Infermiere, Logopedista, Tecnico della fisiopatologia cardiocircolatoria e perfusione cardiovascolare, Tecnico della prevenzione nell'ambiente e nei luoghi di lavoro, Tecnico di neurofisiopatologia, Tecnico ortopedico, Tecnico sanitario di radiologia medica, Tecnico sanitario laboratorio biomedico

Gratuito:

Sì

Modalità:

Online asincrono

Data Inizio:

28 settembre 2026

Data Fine:

27 febbraio 2027

Durata:

2 ore

La crescente digitalizzazione dei processi lavorativi, in particolare nel settore sanitario e nella Pubblica Amministrazione, rende sempre più fondamentale garantire la protezione dei dati personali e la sicurezza delle informazioni. Il Regolamento (UE) 2016/679 (GDPR) e la Direttiva NIS 2 hanno introdotto nuovi obblighi in materia di data protection e cybersicurezza,

richiedendo a professionisti e organizzazioni un costante aggiornamento normativo e operativo.

Il corso si propone di fornire ai partecipanti una panoramica completa dei principali aspetti della normativa vigente, approfondendo il ruolo del Data Protection Officer (DPO), la gestione del Registro delle Attività di Trattamento, la valutazione dei rischi, la gestione dei data breach e le misure di sicurezza informatica da adottare secondo i principi di "privacy by design", "privacy by default" e accountability.

Attraverso un approccio pratico e multidisciplinare saranno inoltre analizzati gli obblighi previsti dalla Direttiva NIS 2, le principali minacce informatiche e le migliori pratiche per la prevenzione degli attacchi cyber, con l'obiettivo di rafforzare le competenze dei partecipanti nella tutela dei dati personali e nella gestione della sicurezza informatica all'interno delle proprie organizzazioni.

PROGRAMMA

RESPONSABILE SCIENTIFICO:

Dr. Carlo Villanacci

Relatori del corso: Avv. Luca Esposito, Avv. Alessandro Boccia

MODULO A: LA NORMATIVA IN TEMA DATA PROTECTION E LA SUA IMPORTANZA NEL CONTESTO DELLA CYBERISCUREZZA

Evoluzione storica;

Le fonti normative;

I principi del GDPR;

Le diverse soggettività.

MODULO B: IL DATA PROTECTION OFFICER - RESPONSABILE DELLA PROTEZIONE DEI DATI E IL SUO RUOLO NELLA SICUREZZA INFORMATICA

DPO: i riferimenti normativi;

Requisiti e qualità professionali del DPO;

I compiti del DPO nel contesto sanitario.

MODULO C: IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO E LE NUOVE ATTIVITÀ DI TRATTAMENTO E IL LORO IMPATTO NEL PERIMETRO DELLA SICUREZZA AZIENDALE

Il Registro delle Attività di Trattamento (RdT);

Il contenuto del Registro delle Attività di Trattamento (Rdт);

Le nuove attività: lo smart working e l'utilizzo dei devices nello svolgimento dell'attività lavorativa.

MODULO D: LA VALUTAZIONE DEI RISCHI NELL'AMBITO DELLA DATA PROTECTION E DELLA CYBERSICUREZZA

I principi in tema di valutazione dei rischi in ambito data protection;

Il Data Protection Impact Assessment (DPIA);

Le altre procedure di risk assessment: Legitimate Interest Assessment (L.I.A.) e Transfer Impact Assessment (T.I.A.).

MODULO E: GLI INCIDENTI DI SICUREZZA E LA LORO GESTIONE

La nozione di data breach;

La procedura di notificazione dell'incidente;

Le forme di tutela degli interessati.

MODULO F: L'IMPORTANZA DI UN EFFICACE PERIMETRO DI SICUREZZA INFORMATICA

La sicurezza informatica by design e by default;

Le misure minime di sicurezza per le pubbliche amministrazioni;

Il principio di accountability nella sicurezza informatica.

MODULO G: ASPETTI REGOLAMENTARI DERIVANTI DALLA DIRETTIVA NIS 2

I principi della Direttiva NIS2;

Gli obblighi di sicurezza per le aziende sanitarie;

Il ruolo del Chief Information Security Officer (CISO);

Risorse e strumenti per l'effettiva implementazione dei principi della Direttiva NIS 2.

MODULO H: GLI ATTACCHI INFORMATICI: METODOLOGIE E TIPOLOGIE DI ATTACCO E BEST PRACTICES PER I DIPENDENTI

Le tipologie più diffuse di attacco informatico e le modalità di veicolazione;

Il phishing: la minaccia più insidiosa;

Raccomandazioni e buone pratiche per i dipendenti della PA.