

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Compliance Integrata Legal Cyber Security

Descrizione	<p>Corso di formazione sulle normative maggiormente impattanti la cybersecurity e la Sicurezza Cibernetica nazionale ed europea, quali il Regolamento (UE) 2016/679 (GDPR), la Direttiva europea 2016/1148, cosiddetta Direttiva NIS recepita in Italia con il D.lgs. 18 maggio 2018, n.65, D.L. 105/2019 in materia di Perimetro di Sicurezza Nazionale Cibernetica.</p>
Obiettivi	<p>Conoscenza della norma nazionale, delle sue applicazioni pratiche e della gestione degli incidenti di sicurezza.</p> <p>In particolare vengono forniti ai partecipanti conoscenze per comprendere:</p> <ul style="list-style-type: none"> • Principi di base della Cyber Security e della Data Protection alla luce delle normative analizzate • Concetti chiave relativi alle normative maggiormente impattanti sulla sicurezza cibernetica nazionale, e, in generale, anche su quella europea e mondiale • Importanza della Cyber Security per la comprensione del Warfare su scala globale
Argomenti principali	<ul style="list-style-type: none"> • Analisi della norma, dei DPCM e delle normative connesse. Cyberwarfare e Legal-Cybersecurity • Implementazione delle misure di sicurezza tecniche, tra SIEM e VAPT. Il punto di vista dell'attaccante • Misure organizzative: gestione terze parti, asset management e l'ottica Risk-based come volano della compliance integrata
Programma di dettaglio	<ul style="list-style-type: none"> • Introduzione alla normativa e ai temi della compliance integrata: framework Cyber Security e contesto giuridico <ul style="list-style-type: none"> ○ Cybersecurity e Data Protection protagonisti del Warfare internazionale ○ Analisi e scenari su Direttiva europea 2016/1148, cosiddetta Direttiva NIS recepita in Italia con il D.lgs. 18 maggio 2018, n.65 ○ Analisi e scenari su Cybersecurity nel Regolamento (UE) 2016/679 (GDPR) ○ D.L. 105/2019 in materia di Perimetro di Sicurezza Nazionale Cibernetica • Misure tecniche: disponibilità, gestione incidenti, visione degli attaccanti <ul style="list-style-type: none"> ○ Misure di sicurezza tecniche per la compliance integrata: GDPR, Perimetro, NIS - Provvedimenti del Garante, Linee Guida ENISA ○ Misure di sicurezza tecniche per la compliance integrata: il punto di vista dell'attaccante ○ Misure di sicurezza organizzative per la compliance integrata: ISO 22301, direttiva NIS e Perimetro, resilienza e disponibilità ○ Esercitazione: la gestione di un incidente di sicurezza • Misure organizzative: gestione Terze parti, Asset e Rischio <ul style="list-style-type: none"> ○ Misure di sicurezza tecniche e organizzative per la compliance integrata: i modelli organizzativi basati sull'analisi del rischio ○ Misure di sicurezza tecniche e organizzative per la compliance integrata: il ruolo del CISO e degli Amministratori di Sistema ○ Misure di sicurezza organizzative per la compliance integrata: la gestione della formazione e delle terze parti ○ Gestione degli asset tra interdipendenze, supply chain e asset management: la compliance a Perimetro e allo standard ISO/IEC 27001
Destinatari	<p>Consulenti in materia giuridica e/o informatica, operatori nei settori della Data Protection e della Cyber Security, e/o dei Sistemi di Gestione aziendali, etc.</p>
Prerequisiti	<p>Ai fini di una maggiore comprensione del corso è consigliato, ma non necessario, aver maturato esperienza di base sull'organizzazione aziendale e sugli aspetti informatici e giuridici (Legal Tech) nel campo della sicurezza dei sistemi, informatica e/o della Data Protection</p>
Durata e frequenza	<p>Corso della durata di 3 giornate (ciascuna tra le 9:00 e le 18:00, comprese pause).</p> <p>Si raccomanda di prevedere del tempo individuale aggiuntivo per consolidare l'apprendimento (attività individuali post-aula, riguardare o completare le esercitazioni e riesaminare la documentazione).</p>

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA Compliance Integrata Legal Cyber Security	
Modalità di partecipazione	<ul style="list-style-type: none"> In presenza in aula con docente* In Virtual Classroom: in web-conference connessi live dal proprio dispositivo con il docente e gli altri allievi In aula remota: in aula a Bari, Milano, etc assieme ad altri discenti, connessi live con l'aula in presenza <p><i>È anche possibile alternare le precedenti modalità</i></p>
Profilo Docenti	<p>Docenti, consulenti e professionisti di estrazione giuridica e/o sicurezza informatica, esperti di Legal Tech, Sistemi di Gestione aziendale ISO 27001 e Privacy GDPR e sicurezza nazionale, in grado di apportare un valore aggiunto esperienziale ai discenti.</p> <p><i>Competenze e certificazioni dei docenti possono essere verificate prima dell'inizio del corso.</i></p>
Metodologia	<p>"Learning by Doing" (imparare facendo) è la metodologia principalmente utilizzata per i corsi abilitanti, integrata dall'uso di supporti didattici di varia natura e dal coinvolgimento immediato dei discenti. In aggiunta alla programmazione, alla qualità dei materiali didattici, e alla professionalità dei docenti, permette alti livelli di apprendimento. Le sessioni teoriche e pratiche si alternano in modo da consentire ai partecipanti il monitoraggio continuo dell'apprendimento.</p> <p>La metodologia include:</p> <ul style="list-style-type: none"> Lezioni frontali interattive con i docenti (da 2 a 4 docenti per ciascuna lezione) Esercitazioni individuali e di gruppo su situazioni e casi reali Materiale didattico individuale Forum di discussione tra studenti attivo h24 anche fuori lezione Test di verifica dell'apprendimento
Materiali didattici	<p>Distribuiti in formato elettronico, tramite piattaforma e-learning, con accesso individuale autenticato attivo per tutta la durata del corso:</p> <ul style="list-style-type: none"> Slide docente proiettate durante il corso Esercitazioni (Casi studio su gestione degli incidenti di sicurezza) Materiale integrativo Questionario di gradimento Quiz finale Attestato <p>Si raccomanda di organizzarsi per avere accesso ai materiali didattici su proprio dispositivo (notebook, Tablet, Smartphone) oppure in forma cartacea, secondo le proprie preferenze.</p>
Test	<p>Al termine del corso viene somministrato un Quiz finale, online, per verificare il livello delle competenze acquisite</p>
Attestati	<p>Attestato di partecipazione al corso rilasciato congiuntamente da ITHUM e ICT Cyber Consulting</p>
Allestimento d'aula*	<p>Aule adeguate e confortevoli per svolgere attività didattiche, dotate di:</p> <ul style="list-style-type: none"> Accesso a Internet Sistema di videoproiezione Lavagna a fogli mobili e/o white-board, con pennarelli colorati Tavoli e sedie preferibilmente mobili (non sedie con ribaltine o bloccate in configurazioni fisse) Climatizzazione e areazione adeguata (preferibilmente indipendente) Raggiungibilità con trasporti pubblici
Numero partecipanti	<p>Normalmente fino a 18 allievi per edizione (per ottimizzare efficacia dell'interazione e dell'apprendimento)</p>
Informazioni e prenotazioni	<p>Mail: formazione@ithum.it Telefono: (+39) 06 2158915 Web: www.ithum.it</p>

* La modalità di partecipazione in aula, fisicamente in presenza, è sospesa per il periodo pandemico!