

<b>CORSO ISO/IEC 27017 e ISO/IEC 27018</b> <b>Codici di condotta per il controllo e la protezione delle informazioni in cloud pubblici</b>	
<b>Descrizione</b>	<p>Corso di formazione sulle Norme <b>ISO/IEC 27017</b> e <b>ISO/IEC 27018</b> sui <b>Codici di condotta per il controllo e la protezione delle informazioni in cloud</b>.</p> <p>Le norme si basano e rinforzano la ISO/IEC 27001 e ISO/IEC 27002 in materia di Gestione della Sicurezza delle Informazioni, e stabiliscono obiettivi di controllo, regole e procedure per implementare misure di protezione delle informazioni e dei dati personali (PII) per i fornitori di servizi cloud.</p>
<b>Contesto</b>	<p>Con la diffusione del cloud computing crescono le preoccupazioni dei clienti di come sono protette le informazioni archiviate nel cloud e dove sono localizzate.</p> <p>La <b>ISO/IEC 27017</b> (Codice di condotta per i controlli di sicurezza delle informazioni basati su ISO/IEC 27002 per i servizi in cloud) e la <b>ISO/IEC 27018</b> (Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici che agiscono come responsabili PII), sono i primi standard a livello internazionale per contribuire a garantire il rispetto dei principi e delle norme privacy, da parte dei providers di public cloud che elaborano dati personali (PII - Personally Identifiable Information) e che agiscono in qualità di Data (PII) Processor.</p> <p>Definiscono delle linee guida basate su ISO/IEC 27002, prendendo in considerazione i requisiti normativi per la protezione dei dati personali che possono essere applicabili nel contesto del panorama dei rischi di sicurezza informatica di un fornitore di servizi public cloud.</p>
<b>Obiettivi</b>	Formare i partecipanti a comprendere i requisiti della ISO/IEC 27017:2015 e della ISO/IEC 27018:2019 nell'ottica degli audit di seconda e terza parte sui Sistemi di Gestione per la Sicurezza delle Informazioni.
<b>Programma di dettaglio</b>	<ul style="list-style-type: none"> <li>• Documenti NITS, ENISA</li> <li>• Circolare Accredia</li> <li>• SaaS, PaaS, IaaS</li> <li>• Analisi dei requisiti della Norma ISO/IEC 27017:2015 e delle relazioni con altre norme</li> <li>• Analisi dei requisiti della Norma ISO/IEC 27018:2019 e delle relazioni con altre norme</li> <li>• Analisi dei riferimenti alla ISO/IEC 29100:2011</li> </ul>
<b>Durata e frequenza</b>	<p>Corso di 2 giornate (16 ore - dalle 9:00 alle 18:00, comprese pause) con test finale alla fine dell'ultima giornata.</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> <p>La frequenza è obbligatoria. Assenze superiori alle 4 ore consecutive possono pregiudicare le competenze acquisite e compromettere il risultato dell'esame finale.</p>
<b>Modalità di partecipazione</b>	In presenza in aula con docente
<b>Destinatari</b>	Consulenti e Progettisti di Sistemi di Gestione per la Sicurezza delle Informazioni, Responsabili della Sicurezza delle Informazioni, Auditor e Lead Auditor della Sicurezza delle Informazioni e di altri schemi ICT, Auditor interni, etc.
<b>Prerequisiti</b>	<p>Obbligatori:</p> <ul style="list-style-type: none"> <li>• Conoscenza ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27006:2015</li> <li>• Conoscenza lingua inglese</li> </ul> <p>Raccomandati:</p> <ul style="list-style-type: none"> <li>• Esperienza nella conduzione di audit di seconda e/o terza parte secondo ISO/IEC 27001:2013</li> </ul>
<b>Numero partecipanti</b>	Fino a 15 persone per edizione ( <i>per ottimizzare l'efficacia dell'interazione e dell'apprendimento</i> )
<b>Metodologia</b>	<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, ed alla professionalità dei docenti, permette alti livelli di apprendimento e di successo all'esame finale.</p> <p>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"> <li>• Studio di situazioni e casi reali</li> <li>• Esercitazioni individuali e di gruppo</li> <li>• Lezioni frontali interattive con i docenti</li> <li>• Materiale didattico individuale</li> </ul>
<b>Materiali didattici</b>	<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"> <li>• Slide proiettate durante il corso</li> <li>• Quaderno a uso didattico contenente tutte le norme necessarie per lo svolgimento del corso (da restituire a fine corso)</li> <li>• Materiale integrativo</li> </ul>

<b>CORSO ISO/IEC 27017 e ISO/IEC 27018</b> <b>Codici di condotta per il controllo e la protezione delle informazioni in cloud pubblici</b>	
	<ul style="list-style-type: none"> <li>Esercitazioni e Casi Studio</li> </ul> <p>Si raccomanda di organizzarsi per portarsi in aula i materiali didattici o su proprio supporto elettronico (notebook, Tablet, Smartphone) oppure in forma cartacea, in base alle proprie preferenze.</p>
<b>Valutazioni</b>	<ul style="list-style-type: none"> <li>Test Ingresso (quiz sulla conoscenza della Norma) – opzionale per chi ha seguito un corso A/LA</li> <li>Test Finale</li> </ul>
<b>Attestati</b>	<ul style="list-style-type: none"> <li>Certificato di frequenza, approvato da ICT Academy® all'interno dell'ISO Academy® Program</li> <li>Per gli Auditor/Lead Auditor della Sicurezza delle Informazioni il corso vale come estensione della qualifica, secondo quanto indicato nella circolare Accredia di riferimento.</li> </ul>
<b>Profilo docenti</b>	<p>Consulenti professionisti, auditor certificati a livello nazionale e/o internazionale da vari registri, formatori esperti, le cui competenze e certificazioni possono essere verificate prima dell'inizio del corso, a garanzia del valore aggiunto e del livello qualitativo dei contenuti</p>
<b>Allestimento d'aula</b>	<p>Aule adeguate e confortevoli per svolgere attività didattiche, dotate di:</p> <ul style="list-style-type: none"> <li>Accesso a Internet</li> <li>Sistema di videoproiezione</li> <li>Lavagna a fogli mobili e/o white-board, con pennarelli colorati</li> <li>Tavoli e sedie preferibilmente mobili (non sedie con ribaltine o bloccate in configurazioni fisse)</li> <li>Climatizzazione e areazione adeguata (preferibilmente indipendente)</li> <li>Raggiungibilità con trasporti pubblici</li> </ul>
<b>Informazioni e prenotazioni</b>	<p>Mail: <a href="mailto:formazione@ithum.it">formazione@ithum.it</a>            Telefono: (+39) 06 2158915            Sito: <a href="http://www.ithum.it/formazione/governance/norma-iso-iec-27017-27018">www.ithum.it/formazione/governance/norma-iso-iec-27017-27018</a></p>