

NORME ISO/IEC 27017:2015 e ISO/IEC 27018:2019

Codici di condotta per il controllo e la protezione delle informazioni in cloud

Descrizione	<p>Corso di formazione sulle Norme ISO/IEC 27017:2015 e ISO/IEC 27018:2019 - Codici di pratica per il controllo e la protezione delle informazioni in cloud e dei dati personali in cloud pubblici.</p> <p>I due standard estendono i controlli definiti nelle ISO/IEC 27001 e ISO/IEC 27002 in materia di Gestione della Sicurezza delle Informazioni in ambito:</p> <ul style="list-style-type: none"> • Servizi in cloud (ISO/IEC 27017) • Servizi in cloud pubblici che includono la protezione di dati personali per i responsabili del trattamento (ISO/IEC 27018)
Contesto	<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, soprattutto nel caso di cloud pubblici che contengono dati personali.</p> <p>Le recenti disposizioni AgID hanno dato enfasi all'importanza dell'estensione delle certificazioni ISO/IEC 27001 ai due nuovi standard ISO/IEC 27017 e ISO/IEC 27018.</p> <p>La ISO/IEC 27017 (<i>Codice di condotta per i controlli di sicurezza delle informazioni basati su ISO/IEC 27002 per i servizi in cloud</i>) e la ISO/IEC 27018 (<i>Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici che agiscono come responsabili PII</i>), sono i primi standard a livello internazionale per contribuire a garantire il rispetto dei principi e delle norme privacy, da parte dei providers di servizi in cloud e dei servizi in public cloud che elaborano dati personali (PII - Personally Identifiable Information) che agiscono in qualità di responsabili del trattamento.</p> <p>I due standard ampliano i controlli della ISO/IEC 27001 e introducono specifici controlli aggiuntivi di cui le organizzazioni devono tener conto per l'estensione dei loro certificati ISO/IEC 27001.</p>
Obiettivi	<p>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</p>
Programma di dettaglio	<ul style="list-style-type: none"> • Documenti NIST, ENISA. AgID • Circolare Accredia 01/2019 • ISO/IEC 27036 • Servizi cloud SaaS, PaaS, IaaS • Analisi dei requisiti dello standard ISO/IEC 27017 e delle relazioni con altre norme • Analisi dei requisiti dello standard ISO/IEC 27018 e delle relazioni con altre norme • Analisi dei riferimenti alla ISO/IEC 29100
Destinatari	<p>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.</p> <p><i>Per gli Auditor/Lead Auditor ISO/IEC 27001 dei Sistemi di Gestione per la Sicurezza delle Informazioni il corso costituisce estensione della qualifica per gli audit sulla ISO/IEC 27017 e ISO/IEC 27018.</i></p>
Prerequisiti	<p>Prerequisiti indispensabili:</p> <ul style="list-style-type: none"> • Conoscenza Norme ISO/IEC 27001:2013 e ISO/IEC 27002:2013 • Conoscenza base della lingua inglese (il corso è in italiano, le norme sono scritte in inglese) • <i>Per l'estensione della qualifica degli Auditor/Lead Auditor ISO/IEC 27001 è necessaria l'attestazione rilasciata da Organismo di Certificazione delle Competenze accreditato (ad es. AICQ SICEV)</i> <p>Prerequisiti preferibili:</p> <ul style="list-style-type: none"> • Esperienza nella conduzione di audit secondo ISO/IEC 27001 • Conoscenza delle Norme ISO/IEC 17021-1:2015 e ISO 19011:2018

NORME ISO/IEC 27017:2015 e ISO/IEC 27018:2019

Codici di condotta per il controllo e la protezione delle informazioni in cloud

Durata e frequenza	<p>Corso di 2 giornate (tra le 9:00 e le 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>
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 <p><i>È anche possibile alternare le precedenti modalità</i></p>
Profilo docenti	<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> <p>Il docente primario, responsabile e progettista area ISO è Fabrizio CIRILLI (Linkedin)</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 e di successo all'esame finale. 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 • Esercitazioni individuali e di gruppo • Studio di situazioni e casi reali • Materiale didattico individuale • Test finale
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 proiettate durante il corso • Materiale integrativo di approfondimento <p><i>Le credenziali per il primo accesso vengono inviate per mail agli allievi</i></p> <p>Durante le lezioni vengono messe a disposizione le Norme a uso didattico (da restituire a fine corso)</p>
Valutazioni	<ul style="list-style-type: none"> • Test Ingresso (conoscenza della ISO/IEC 27001) – <i>opzionale per chi ha seguito un corso A/LA</i> • Test Finale
Attestati	<ul style="list-style-type: none"> • Attestato di frequenza, approvato da ICT Academy® all'interno dell'ISO Academy® Program • <i>Per gli Auditor/Lead Auditor ISO/IEC 27001 della Sicurezza delle Informazioni il corso vale come estensione della qualifica, secondo quanto indicato nella circolare Accredia di riferimento.</i>
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)

NORME ISO/IEC 27017:2015 e ISO/IEC 27018:2019**Codici di condotta per il controllo e la protezione delle informazioni in cloud**

	<ul style="list-style-type: none">• Raggiungibilità con trasporti pubblici
Numero partecipanti	Fino a 15 persone per edizione <i>(per ottimizzare l'efficacia dell'interazione e dell'apprendimento)</i>
Informazioni e prenotazioni	Mail: formazione@ithum.it Telefono: (+39) 06 2158915 Sito: www.ithum.it/formazione/governance/norma-iso-iec-27017-27018

ithum®