	4. Verifiche di sorveglianza condotte nel primo e nel secondo anno al fine di verificare la continua conformità dell'organizzazione allo standard, 5. Un audit di ri-certificazione nel terzo anno prima della scadenza della certificazione. La certificazione potrà essere successivamente rinnovata per successivi periodi triennali (ENISA 2013). 6. Il certificato può essere revocato o sospeso se la revisione annuale lo giustifica. L'ente certificante sospende la certificazione nei casi in cui, ad esempio, il sistema di gestione certificata del cliente ha persistentemente o gravemente mancato di soddisfare i requisiti di certificazione, inclusi i requisiti per l'efficacia del sistema di gestione, il cliente certificato non consente di effettuare audit di sorveglianza o ri-certificazione alle frequenze richieste o il cliente certificato ha volontariamente richiesto una sospensione (ENISA 2013).
Accreditamento dell'organismo di certificazione	ISO indirizza i propri clienti ad enti di certificazione accreditati, che hanno acquisito una competenza indipendente e riconosciuta da parte di un Organismo di Accreditamento. Gli organismi di certificazione accreditati devono essere in grado di offrire una certificazione conforme alla norma ISO/IEC 17021-1, che contiene principi e requisiti per la competenza, la coerenza e l' imparzialità degli organismi che forniscono audit e certificazione di tutti i tipi di sistemi di gestione e alla norma ISO/IEC 27006 che stabilisce i requisiti per gli organismi che forniscono audit e certificazione dei sistemi di gestione della sicurezza delle informazioni (documento di criteri per l' accreditamento, peer assessment o altri processi di audit) (ISO 2017).
Durata del processo	La durata della procedura di certificazione nel suo complesso dipende dall'ambito della certificazione. Secondo uno studio passato, il periodo di tempo necessario alle imprese oggetto dell'indagine per prepararsi alla certificazione variava tra i 3 e i 18 mesi, la maggior parte delle imprese ha richiesto dai 6 ai 12 mesi per completare la preparazione. Il processo di certificazione in sé non ha superato la settimana.
Monitoraggio post-certificazione	Dipende dall' organismo che fornisce la certificazione
Periodo di validità della certificazione	3 anni
Risorse	Non specificato
Certificazioni rilasciate	Nel 2015 sono stati rilasciati in tutto il mondo 27536 certificati, tenendo conto solo di quelli rilasciati da organismi di certificazione accreditati (ISO 2015).

9.6 A.6 – Certificazione basata su ISO/IEC 27018

Ambito	Descrizione
Campo di applicazione e oggetto	Il codice di condotta ISO/IEC 27018:2014 stabilisce gli obiettivi di controllo, i controlli e le linee guida comunemente accettati per l'attuazione di misure volte a proteggere le informazioni personali (PII) in conformità ai principi di riservatezza contenuti nella norma ISO/IEC 29100 per l'ambiente di cloud computing pubblico. Specifica le linee guida basate sulla norma ISO/IEC 27002, tenendo conto dei requisiti normativi per la protezione della PII che potrebbero essere applicabili nel contesto