FAQ ISO27001

Domanda	Risposta	Note MIZAR
1. Che cos'è l'ISO 27001?	ISO 27001 è uno standard internazionale emesso dall'International Standardization Organization (ISO), che definisce i sistemi di gestione della sicurezza delle informazioni. Il suo titolo completo è ISO/IEC 27001:2022. Questo standard è ora diventato uno standard internazionale leader per la sicurezza delle informazioni.	
2. Cosa si ottiene implementando la ISO 27001?	L'implementazione della norma ISO 27001 riduce i rischi legati alla riservatezza, alla disponibilità e all'integrità delle informazioni in un'organizzazione. Aiuta inoltre l'organizzazione a raggiungere la conformità con la legislazione che regola la protezione delle informazioni riservate, la protezione dei sistemi informativi, la protezione dei dati personali, ecc., che sono già in vigore nella maggior parte dei paesi. Infine, l'implementazione dello standard dovrebbe ridurre i costi aziendali a causa di un minor numero di incidenti e migliorare il marketing grazie alla pubblicità che può essere ottenuta con lo standard.	Le motivazioni a fianco riportate hanno spinto la MIZAR ad intraprendere il percorso della certificazione ISO27001 che si concluderà con il passaggio nella nuova sede dove si è puntato molto sulla sicurezza delle informazioni
3. Qual è la differenza tra ISO 27001 e ISO 27002?	Lo standard internazionale ISO 27002 (nome completo: ISO/IEC 27002:2022) definisce le linee guida per l'implementazione dei controlli elencati in ISO 27001. ISO 27001 specifica i controlli che possono essere utilizzati per ridurre i rischi per la sicurezza e ISO 27002 fornisce dettagli su come implementare questi controlli. Le organizzazioni possono ottenere la certificazione ISO 27001, ma non ISO 27002.	
4. Abbiamo implementato la ISO 9001; una parte può essere utilizzata per ISO 27001?	Assolutamente! Alcune parti della ISO 27001 e della ISO 9001 sono virtualmente le stesse, ad esempio la gestione della documentazione, gli audit interni, il riesame della direzione e le azioni correttive. Se le suddette procedure sono già utilizzate per la ISO 9001, possono essere utilizzate anche per la ISO 27001 con solo lievi modifiche. In altre parole, le organizzazioni che hanno già implementato la ISO 9001 avranno un lavoro più semplice implementando la ISO 27001	
5. Quanto tempo ci vuole per implementare la ISO 27001?	Questo dipende davvero da un gran numero di fattori, ma in generale, le organizzazioni più piccole potrebbero aver bisogno di 3-6 mesi, le organizzazioni con un massimo di 500 persone avranno bisogno di 8-12 mesi e le organizzazioni più grandi 12 mesi o più.	
6. Abbiamo sentito che la ISO 27001 è accompagnata da un'ampia	È vero che la ISO 27001 richiede alcuni documenti obbligatori, ma il loro numero dipende dalla dimensione e dalla complessità dell'organizzazione: una piccola organizzazione senza grandi requisiti di sicurezza avrà bisogno solo di una dozzina di documenti; una grande banca può richiedere diverse centinaia di documenti. L'importante nella stesura	Alcuni dei documenti e delle registrazioni ISO 27001 obbligatori: Documento di ambito ISMS

Domanda	Risposta	Note MIZAR
documentazione che non farà altro che rallentare la nostra attività quotidiana: è vero?	della documentazione è definire solo le regole realmente necessarie all'organizzazione, per non rallentare l'operatività aziendale.	Politica di sicurezza delle informazioni Rapporto di valutazione dei rischi Dichiarazione di applicabilità Rapporto di audit interno
7.Quali documenti non sono obbligatori per la ISO27001?	Esistono numerosi documenti ISO 27001 non obbligatori che però possono essere utilizzati per l'implementazione, in particolare per i controlli di sicurezza dell'allegato A. L'azienda deve valutare quali dei seguenti documenti ritiene utili. Procedura per il controllo dei documenti e delle registrazioni (punto 7.5, controllo A.5.33) Procedura per l'audit interno (clausola 9.2) Procedura per le azioni correttive (clausola 10.2) Politica di classificazione delle informazioni (controlli A.5.10, A.5.12 e A.5.13) Politica di trasferimento delle informazioni (controllo A.5.14) Politica di controllo degli accessi (controllo A.5.15) Criteri password (controlli A.5.16, A.5.17 e A.8.5) Politica di sicurezza dei fornitori (controlli A.5.19, A.5.21, A.5.22 e A.5.23) Piano di ripristino di emergenza (controlli A.5.29, A.5.30 e A.8.14) Criteri per dispositivi mobili, telelavoro e lavoro da casa (controlli A.6.7, A.7.8, A.7.9 e A.8.1) Procedure per lavorare in aree sicure (controlli A.7.4 e A.7.6) Politica Clear Desk e Clear Screen (controllo A.7.7) Criterio BYOD (Bring Your Own Device) (controlli A.7.8 e A.8.1) Politica di smaltimento e distruzione (controlli A.7.10, A.7.14 e A.8.10) Politica di backup (controllo A.8.13) Politica di crittografia (controllo A.8.24) Politica di gestione delle modifiche (controllo A.8.32)	

Domanda	Risposta	Note MIZAR
8. In che modo la revisione ISO 27001 2022 influisce sui documenti e sui record obbligatori?	La nuova ISO 27001:2022 porta buone notizie quando si tratta di documentazione: • Questa nuova revisione richiede meno documenti obbligatori rispetto alla vecchia revisione ISO 27001:2013. • Anche se ci sono 11 nuovi controlli di sicurezza nella revisione 2022, non è necessario scrivere nuovi documenti a causa loro - è sufficiente includere nuove sezioni su tali controlli nei documenti che hai già scritto per la revisione 2013 dello standard	
9.Quali sono i nuovi controlli di sicurezza inseriti nella ISO27002?	• A.5.7 Informazioni sulle minacce- Può essere gestito nella Procedura di gestione degli incidenti • A.5.23 Sicurezza delle informazioni per l'utilizzo dei servizi cloud - Può essere gestito nella Politica di sicurezza dei fornitori • A.5.30 Preparazione ICT per la continuità operativa - Può essere gestito nel Piano di ripristino di emergenza • A.7.4 Monitoraggio della sicurezza fisica - Può essere gestito nelle Procedure per lavorare in aree sicure • A.8.9 Gestione della configurazione - Può essere gestito nelle Procedure di sicurezza per il reparto IT • A.8.10 Cancellazione delle informazioni - Può essere gestito nella Politica di smaltimento e distruzione • A.8.11 Mascheramento dei dati - Può essere gestito nella Politica di sviluppo sicuro • A.8.12 Prevenzione della perdita di dati - Può essere gestito nelle Procedure di sicurezza per il reparto IT • A.8.16 Attività di monitoraggio - Può essere gestito nelle Procedure di sicurezza per il reparto IT • A.8.23 Filtraggio del Web - Può essere gestito nelle Procedure di sicurezza per il reparto IT • A.8.28 Codifica sicura - Può essere gestito nella Politica di sviluppo sicuro	