**MODELLO DI CHECKLIST DEI CONTROLLI ISO 27001**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SEZIONE****CATEGORIA** | **REQUISITO/ATTIVITÀ** | **ASSEGNATO A** | **CONFORME?** | **DATA DELL'ULTIMO AGGIORNAMENTO** |
| ***5. Politiche di sicurezza delle informazioni*** |
| 5.1 | Sono state definite politiche della sicurezza. |   |   |   |
| 5.2 | Tutte le politiche sono state approvate dai vertici dirigenziali. |   |   |   |
| 5.3 | La conformità è documentata. |   |   |   |
| ***6. Organizzazione della sicurezza delle informazioni*** |
| 6.1 | Ruoli e responsabilità sono stati definiti. |   |  |  |
| 6.2 | Le mansioni sono state correttamente assegnate a persone diverse. |   |  |  |
| 6.3 | È stato contattato l'ente / l'autorità che deve effettuare la verifica della conformità. |   |  |  |
| 6.4 | Sono stati contattati i gruppi di interesse speciali che si occupano di conformità. |   |  |  |
| 6.5 | La sicurezza delle informazioni nella gestione dei progetti è documentata. |   |  |  |
| 6.6 | È stata definita una politica per i dispositivi mobili. |   |  |  |
| 6.7 | È stata definita una politica per il lavoro a distanza. |   |  |  |
| ***7. Sicurezza nelle risorse umane*** |
| 7.1 | È stata definita una politica per la valutazione dei dipendenti prima dell'assunzione. |   |  |  |
| 7.2 | È stata definita una politica HR per i termini e le condizioni di impiego. |   |  |  |
| 7.3 | È stata definita una politica che stabilisca le responsabilità a livello dirigenziale.  |   |  |  |
| 7.4 | È stata definita una politica per la sensibilizzazione e la formazione in materia di sicurezza delle informazioni. |   |  |  |
| 7.5 | È stata definita una politica per i procedimenti disciplinari in materia di sicurezza delle informazioni. |   |  |  |
| 7.6 | È stata definita una politica in materia di sicurezza delle informazioni in caso di cessazione o di modifica del rapporto di lavoro. |   |  |  |
| ***8. Gestione degli asset*** |
| 8.1 | Elenco completo degli asset inventariati. |   |  |  |
| 8.2 | Elenco completo della proprietà degli asset. |   |  |  |
| 8.3 | È stata definita una politica per "l'uso accettabile" degli asset. |   |  |  |
| 8.4 | È stata definita una politica per il reso degli asset. |   |  |  |
| 8.5 | È stata definita una politica per la classificazione delle informazioni.  |   |  |  |
| 8.6 | È stata definita una politica per l'etichettatura delle informazioni. |   |  |  |
| 8.7 | È stata definita una politica per la gestione degli asset. |   |  |  |
| 8.8 | È stata definita una politica per la gestione dei supporti multimediali rimovibili. |   |  |  |
| 8.9 | È stata definita una politica per lo smaltimento dei supporti multimediali. |   |  |  |
| 8.10 | È stata definita una politica per il trasferimento dei supporti multimediali fisici. |   |  |  |
| ***9. Controllo degli accessi*** |
| 9.1 | È stata definita una politica per la registrazione e l'annullamento della registrazione degli asset degli utenti. |   |  |  |
| 9.2 | È stata definita una politica per il provisioning degli accessi degli utenti. |   |  |  |
| 9.3 | È stata definita una politica per la gestione dei diritti di accesso con privilegi. |   |  |  |
| 9.4 | È stata definita una politica per la gestione delle informazioni di autenticazione segrete degli utenti. |   |  |  |
| 9.5 | È stata definita una politica per la revisione dei diritti di accesso degli utenti. |   |  |  |
| 9.6 | È stata definita una politica per la rimozione o l'adeguamento dei diritti di accesso. |   |  |  |
| 9.7 | È stata definita una politica per l'utilizzo delle informazioni di autenticazione segrete. |   |  |  |
| 9.8 | È stata definita una politica per le limitazioni di accesso alle informazioni. |   |  |  |
| 9.9 | È stata definita una politica per le procedure di log-in sicuro. |   |  |  |
| 9.10 | È stata definita una politica per i sistemi di gestione delle password. |   |  |  |
| 9.11 | È stata definita una politica per l'utilizzo di programmi di utility con privilegi. |   |  |  |
| 9.12 | È stata definita una politica per il controllo degli accessi al codice sorgente del programma. |   |  |  |
| ***10. Crittografia*** |
| 10.1 | È stata definita una politica per l'utilizzo dei controlli di crittografia. |   |  |  |
| 10.2 | È stata definita una politica per la gestione delle chiavi. |   |  |  |
| ***11. Sicurezza fisica e ambientale*** |
| 11.1 | È stata definita una politica per la sicurezza fisica perimetrale. |   |  |  |
| 11.2 | È stata definita una politica per i controlli degli ingressi fisici. |   |  |  |
| 11.3 | È stata definita una politica per la messa in sicurezza degli uffici, delle sale e delle infrastrutture. |   |  |  |
| 11.4 | È stata definita una politica per la protezione dalle minacce esterne e ambientali. |   |  |  |
| 11.5 | È stata definita una politica per accedere alle aree protette. |   |  |  |
| 11.6 | È stata definita una politica per le aree di consegna e carico. |   |  |  |
| 11.7 | È stata definita una politica per la protezione delle apparecchiature e per la loro ubicazione in luoghi sicuri. |   |  |  |
| 11.8 | È stata definita una politica per il supporto dei servizi di pubblica utilità. |   |  |  |
| 11.9 | È stata definita una politica per la sicurezza dei cablaggi. |   |  |  |
| 11.10 | È stata definita una politica per la manutenzione delle apparecchiature. |   |  |  |
| 11.11 | È stata definita una politica per l'eliminazione degli asset. |   |  |  |
| 11.12 | È stata definita una politica per la sicurezza delle apparecchiature e degli asset off-premises. |   |  |  |
| 11.13 | Smaltimento sicuro o riutilizzo delle apparecchiature. |   |  |  |
| 11.14 | È stata definita una politica per le apparecchiature degli utenti non presidiate. |   |  |  |
| 11.15 | È stata definita una politica "clear desk" e "clear screen". |   |  |  |
| ***12. Sicurezza delle operazioni*** |
| 12.1 | È stata definita una politica per le procedure operative documentate. |   |  |  |
| 12.2 | È stata definita una politica per la gestione delle modifiche. |   |  |  |
| 12.3 | È stata definita una politica per la gestione della capacità. |   |  |  |
| 12.4 | È stata definita una politica per la separazione tra ambiente di sviluppo, di test e operativo. |   |  |  |
| 12.5 | È stata definita una politica per i controlli antimalware. |   |  |  |
| 12.6 | È stata definita una politica per il backup dei sistemi. |   |  |  |
| 12.7 | È stata definita una politica per il backup delle informazioni. |   |  |  |
| 12.8 | È stata definita una politica per la registrazione degli eventi. |   |  |  |
| 12.9 | È stata definita una politica per la protezione delle informazioni dei registri. |   |  |  |
| 12.10 | È stata definita una politica per i registri amministrativi e operativi. |   |  |  |
| 12.11 | È stata definita una politica per la sincronizzazione dell'orologio di sistema. |   |  |  |
| 12.12 | È stata definita una politica per l'installazione di software nei sistemi operativi. |   |  |  |
| 12.13 | È stata definita una politica per la gestione delle vulnerabilità tecniche. |   |  |  |
| 12.14 | È stata definita una politica per le restrizioni all'installazione di software. |   |  |  |
| 12.15 | È stata definita una politica per il controllo degli audit dei sistemi informativi. |   |  |  |
| ***13. Sicurezza delle comunicazioni*** |
| 13.1 | È stata definita una politica per i controlli di rete. |   |  |  |
| 13.2 | È stata definita una politica per la sicurezza dei servizi di rete. |   |  |  |
| 13.3 | È stata definita una politica per la segmentazione delle reti. |   |  |  |
| 13.4 | È stata definita una politica per i criteri e le procedure di trasferimento delle informazioni. |   |  |  |
| 13.5 | È stata definita una politica per stipulare accordi sul trasferimento delle informazioni. |   |  |  |
| 13.6 | È stata definita una politica per la messaggistica elettronica. |   |  |  |
| 13.7 | È stata definita una politica per gli accordi di riservatezza e non divulgazione. |   |  |  |
| 13.8 | È stata definita una politica per l'acquisizione, lo sviluppo e la manutenzione dei sistemi. |   |  |  |
| ***14. Acquisizione, sviluppo e manutenzione dei sistemi*** |
| 14.1 | È stata definita una politica per l'analisi e le specifiche dei requisiti di sicurezza delle informazioni. |   |  |  |
| 14.2 | È stata definita una politica per proteggere i servizi delle applicazioni sulle reti pubbliche. |   |  |  |
| 14.3 | È stata definita una politica per proteggere le transazioni dei servizi delle applicazioni. |   |  |  |
| ***15. Relazioni con i fornitori*** |
| 15.1 | È stata definita una politica per le relazioni con i fornitori. |   |  |  |
| ***16. Gestione degli incidenti di sicurezza delle informazioni*** |
| 16.1 | È stata definita una politica per la gestione della sicurezza delle informazioni. |   |  |  |
| ***17. Aspetti della sicurezza delle informazioni nella gestione della continuità operativa*** |
| 17.1 | È stata definita una politica delle ridondanze. |   |  |  |
| ***18. Conformità*** |
| 18.1 | È stata definita una politica per l'identificazione degli obblighi legali e contrattuali applicabili. |   |  |  |
| 18.2 | È stata definita una politica per i diritti di proprietà intellettuale. |   |  |  |
| 18.3 | È stata definita una politica per la protezione dei record. |   |  |  |
| 18.4 | È stata definita una politica per la privacy e la protezione dei dati personali (PII). |   |  |  |
| 18.5 | È stata definita una politica per la regolamentazione dei controlli di crittografia. |   |  |  |
| 18.6 | È stata definita una politica per la conformità ai criteri e agli standard di sicurezza. |   |  |  |
| 18.7 | È stata definita una politica per l'esame della conformità tecnica. |   |  |  |

**DICHIARAZIONE DI NON RESPONSABILITÀ**

Qualsiasi articolo, modello o informazione sono forniti da Smartsheet sul sito web solo come riferimento. Pur adoperandoci a mantenere le informazioni aggiornate e corrette, non offriamo alcuna garanzia o dichiarazione di alcun tipo, esplicita o implicita, relativamente alla completezza, l’accuratezza, l’affidabilità, l’idoneità o la disponibilità rispetto al sito web o le informazioni, gli articoli, i modelli o della relativa grafica contenuti nel sito. Qualsiasi affidamento si faccia su tali informazioni, è pertanto strettamente a proprio rischio.

Questo modello è fornito solo come esempio. Questo modello non è in alcun modo concepito come consiglio legale o di conformità. Gli utenti del modello devono individuare tra le varie informazioni quelle necessarie e adeguate ai propri obiettivi.