|  |  |  |
| --- | --- | --- |
|  | **PUNTI DI CONTROLLO ANNEX A NORMA 27001:2022** | |
| **5** | **Controlli organizzativi** | **Descrizione del controllo** |
| 5,1 | Politiche per la sicurezza delle informazioni | La politica di sicurezza delle informazioni e le politiche specifiche per argomento dovrebbero essere definite, approvate dalla direzione, pubblicate, comunicate e approvate dal personale pertinente e dalle parti interessate pertinenti e riviste a intervalli pianificati e se si verificano cambiamenti significativi. |
| 5.2 | Ruoli e responsabilità della sicurezza delle informazioni | I ruoli e le responsabilità della sicurezza delle informazioni dovrebbero essere definiti e assegnati in base alle esigenze dell'organizzazione. |
| 5.3 | Separazione dei compiti | I doveri in conflitto e le aree di responsabilità in conflitto dovrebbero essere separati. |
| 5.4 | Responsabilità di gestione | La direzione dovrebbe richiedere a tutto il personale di applicare la sicurezza delle informazioni in conformità con la politica di sicurezza delle informazioni stabilita, le politiche e le procedure specifiche dell'argomento dell'organizzazione. |
| 5.5 | Contatto con le autorità | L'organizzazione dovrebbe stabilire e mantenere i contatti con le autorità competenti. |
| 5.6 | Contatti con gruppi di interesse speciale | L'organizzazione dovrebbe stabilire e mantenere contatti con gruppi di interesse speciale o altri forum di sicurezza specializzati e associazioni professionali. |
| 5.7 | Intelligence sulle minacce | Le informazioni relative alle minacce alla sicurezza delle informazioni dovrebbero essere raccolte e analizzate per produrre informazioni sulle minacce. |
| 5.8 | Sicurezza delle informazioni nella gestione dei progetti | La sicurezza delle informazioni dovrebbe essere integrata nella gestione dei progetti. |
| 5.9 | Inventario di informazioni e altri beni associati | Dovrebbe essere sviluppato e mantenuto un inventario delle informazioni e delle altre risorse associate, compresi i proprietari. |
| 5.10 | Uso accettabile delle informazioni e di altre risorse associate | Le regole per l'uso accettabile e le procedure per la gestione delle informazioni e delle altre risorse associate dovrebbero essere identificate, documentate e implementate. |
| 5.11 | Restituzione di beni | Il personale e le altre parti interessate, a seconda dei casi, dovrebbero restituire tutti i beni dell'organizzazione in loro possesso in caso di modifica o risoluzione del rapporto di lavoro, contratto o accordo. |
| 5.12 | Classificazione delle informazioni | Le informazioni dovrebbero essere classificate in base alle esigenze di sicurezza delle informazioni dell'organizzazione sulla base di riservatezza, integrità, disponibilità e requisiti pertinenti delle parti interessate. |
| 5.13 | Etichettatura delle informazioni | Un insieme appropriato di procedure per l'etichettatura delle informazioni dovrebbe essere sviluppato e implementato in conformità con lo schema di classificazione delle informazioni adottato dall'organizzazione. |
| 5.14 | Trasferimento di informazioni | Dovrebbero essere in vigore regole, procedure o accordi per il trasferimento delle informazioni per tutti i tipi di strutture di trasferimento all'interno dell'organizzazione e tra l'organizzazione e altre parti. |
| 5.15 | Controllo accessi | Le regole per controllare l'accesso fisico e logico alle informazioni e ad altre risorse associate dovrebbero essere stabilite e implementate sulla base dei requisiti di sicurezza aziendale e delle informazioni. |
| 5.16 | Gestione dell'identità | L'intero ciclo di vita delle identità dovrebbe essere gestito. |
| 5.17 | Informazioni di autenticazione | L'allocazione e la gestione delle informazioni di autenticazione dovrebbero essere controllate da un processo di gestione, compresa la consulenza al personale sul trattamento appropriato delle informazioni di autenticazione. |
| 5.18 | Diritti di accesso | I diritti di accesso alle informazioni e ad altre risorse associate devono essere forniti, riesaminati, modificati e rimossi in conformità con la politica specifica dell'argomento e le regole per il controllo degli accessi dell'organizzazione. |
| 5.19 | Sicurezza delle informazioni nei rapporti con i fornitori | Devono essere definiti e implementati processi e procedure per gestire i rischi per la sicurezza delle informazioni associati all'uso dei prodotti o servizi del fornitore. |
| 5.20 | Affrontare la sicurezza delle informazioni negli accordi con i fornitori | I requisiti di sicurezza delle informazioni pertinenti dovrebbero essere stabiliti e concordati con ciascun fornitore in base al tipo di rapporto con il fornitore. |
| 5.21 | Gestire la sicurezza delle informazioni nella filiera ICT | Dovrebbero essere definiti e implementati processi e procedure per gestire i rischi per la sicurezza delle informazioni associati alla catena di fornitura di prodotti e servizi ICT. |
| 5.22 | Monitoraggio, revisione e gestione del cambiamento dei servizi dei fornitori | L'organizzazione dovrebbe monitorare, rivedere, valutare e gestire regolarmente i cambiamenti nelle pratiche di sicurezza delle informazioni dei fornitori e nell'erogazione dei servizi. |
| 5.23 | Sicurezza delle informazioni per l'utilizzo dei servizi cloud | I processi per l'acquisizione, l'utilizzo, la gestione e l'uscita dai servizi cloud devono essere stabiliti in conformità con i requisiti di sicurezza delle informazioni dell'organizzazione. |
| 5.24 | Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni | L'organizzazione dovrebbe pianificare e prepararsi per la gestione degli incidenti di sicurezza delle informazioni definendo, stabilendo e comunicando processi, ruoli e responsabilità di gestione degli incidenti di sicurezza delle informazioni. |
| 5.25 | Valutazione e decisione sugli eventi di sicurezza delle informazioni | L'organizzazione dovrebbe valutare gli eventi di sicurezza delle informazioni e decidere se devono essere classificati come incidenti di sicurezza delle informazioni. |
| 5.26 | Risposta agli incidenti di sicurezza delle informazioni | Gli incidenti di sicurezza delle informazioni dovrebbero essere risolti secondo le procedure documentate. |
| 5.27 | Imparare dagli incidenti di sicurezza delle informazioni | Le conoscenze acquisite dagli incidenti relativi alla sicurezza delle informazioni dovrebbero essere utilizzate per rafforzare e migliorare i controlli sulla sicurezza delle informazioni. |
| 5.28 | Raccolta delle prove | L'organizzazione dovrebbe stabilire e attuare procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove relative agli eventi di sicurezza delle informazioni. |
| 5.29 | Sicurezza delle informazioni durante l'interruzione | L'organizzazione dovrebbe pianificare come mantenere la sicurezza delle informazioni a un livello appropriato durante l'interruzione. |
| 5.30 | Prontezza ICT per la continuità aziendale | La prontezza delle ICT dovrebbe essere pianificata, implementata, mantenuta e testata sulla base degli obiettivi di continuità operativa e dei requisiti di continuità delle ICT. |
| 5.31 | Requisiti legali, statutari, regolamentari e contrattuali | I requisiti legali, statutari, normativi e contrattuali rilevanti per la sicurezza delle informazioni e l'approccio dell'organizzazione per soddisfare tali requisiti devono essere identificati, documentati e tenuti aggiornati. |
| 5.32 | Diritti di proprietà intellettuale | L'organizzazione dovrebbe attuare procedure appropriate per proteggere i diritti di proprietà intellettuale. |
| 5.33 | Protezione dei registri | Le registrazioni dovrebbero essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato. |
| 5.34 | Privacy e tutela delle PII (*Personally Identifiable Information*) | L'organizzazione dovrebbe identificare e soddisfare i requisiti relativi alla conservazione della privacy e alla protezione delle PII secondo le leggi e i regolamenti applicabili e i requisiti contrattuali. |
| 5.35 | Revisione indipendente della sicurezza delle informazioni | L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e alla sua implementazione, comprese le persone, i processi e le tecnologie, dovrebbe essere rivisto in modo indipendente a intervalli pianificati o quando si verificano cambiamenti significativi. |
| 5.36 | Conformità a politiche, regole e standard per la sicurezza delle informazioni | La conformità con la politica di sicurezza delle informazioni dell'organizzazione, le politiche, le regole e gli standard specifici dell'argomento dovrebbe essere riesaminata regolarmente. |
| 5.37 | Procedure operative documentate | Le procedure operative per le strutture di elaborazione delle informazioni dovrebbero essere documentate e messe a disposizione del personale che ne ha bisogno. |
| **6** | **Controlli delle persone** | |
| 6.1 | Proiezione | I controlli di background su tutti i candidati a diventare personale dovrebbero essere effettuati prima dell'ingresso nell'organizzazione e su base continuativa, tenendo conto delle leggi, dei regolamenti e dell'etica applicabili ed essere proporzionati ai requisiti aziendali, alla classificazione delle informazioni a cui accedere e ai rischi percepiti. |
| 6.2 | Termini e condizioni di lavoro | Gli accordi contrattuali di lavoro dovrebbero indicare le responsabilità del personale e dell'organizzazione per la sicurezza delle informazioni. |
| 6.3 | Sensibilizzazione, istruzione e formazione alla sicurezza delle informazioni | Il personale dell'organizzazione e le parti interessate pertinenti dovrebbero ricevere un'adeguata sensibilizzazione alla sicurezza delle informazioni, istruzione e formazione e aggiornamenti regolari della politica di sicurezza delle informazioni dell'organizzazione, delle politiche e delle procedure specifiche per argomento, come pertinenti per la loro funzione lavorativa. |
| 6.4 | Processo disciplinare | Un processo disciplinare dovrebbe essere formalizzato e comunicato per intraprendere azioni contro il personale e altre parti interessate pertinenti che hanno commesso una violazione della politica di sicurezza delle informazioni. |
| 6.5 | Responsabilità dopo la cessazione o il cambio di rapporto di lavoro | Le responsabilità e gli obblighi in materia di sicurezza delle informazioni che rimangono validi dopo la cessazione o il cambio di rapporto di lavoro devono essere definiti, applicati e comunicati al personale pertinente e alle altre parti interessate. |
| 6.6 | Accordi di riservatezza o non divulgazione | Gli accordi di riservatezza o di non divulgazione che riflettano le esigenze dell'organizzazione per la protezione delle informazioni dovrebbero essere identificati, documentati, riesaminati regolarmente e firmati dal personale e dalle altre parti interessate pertinenti. |
| 6.7 | Lavoro a distanza | Le misure di sicurezza dovrebbero essere implementate quando il personale lavora in remoto per proteggere le informazioni a cui ha accesso, elaborate o archiviate al di fuori dei locali dell'organizzazione. |
| 6.8 | Segnalazione di eventi di sicurezza delle informazioni | L'organizzazione dovrebbe fornire un meccanismo che consenta al personale di segnalare tempestivamente eventi di sicurezza delle informazioni osservati o sospetti attraverso canali appropriati. |
| **7** | **Controlli fisici** | |
| 7.1 | Perimetri di sicurezza fisica | I perimetri di sicurezza devono essere definiti e utilizzati per proteggere le aree che contengono informazioni e altre risorse associate. |
| 7.2 | Ingresso fisico | Le aree sicure dovrebbero essere protette da adeguati controlli di accesso e punti di accesso. |
| 7.3 | Messa in sicurezza di uffici, locali e strutture | La sicurezza fisica per uffici, stanze e strutture dovrebbe essere progettata e implementata. |
| 7.4 | Monitoraggio della sicurezza fisica | I locali dovrebbero essere costantemente monitorati per l'accesso fisico non autorizzato. |
| 7.5 | Protezione contro le minacce fisiche e ambientali | Dovrebbe essere progettata e implementata la protezione contro le minacce fisiche e ambientali, come i disastri naturali e altre minacce fisiche intenzionali o non intenzionali all'infrastruttura. |
| 7.6 | Lavorare in aree sicure | Dovrebbero essere progettate e attuate misure di sicurezza per lavorare in aree sicure. |
| 7.7 | Scrivania e schermo protetti | Dovrebbero essere definite e opportunamente applicate regole chiare per documenti e supporti di archiviazione rimovibili e regole chiare per lo schermo per le strutture di elaborazione delle informazioni. |
| 7.8 | Posizionamento e protezione delle apparecchiature | L'attrezzatura deve essere posizionata in modo sicuro e protetto. |
| 7.9 | Sicurezza dei beni fuori sede | Le risorse fuori sede dovrebbero essere protette. |
| 7.10 | Supporti di memorizzazione | I supporti di memorizzazione dovrebbero essere gestiti durante il loro ciclo di vita di acquisizione, uso, trasporto e smaltimento in conformità con lo schema di classificazione dell'organizzazione e i requisiti di gestione. |
| 7.11 | Utilità di supporto | Le strutture di elaborazione delle informazioni dovrebbero essere protette da interruzioni di corrente e altre interruzioni causate da guasti nelle utenze di supporto. |
| 7.12 | Sicurezza del cablaggio | I cavi che trasportano alimentazione, dati o servizi informativi di supporto devono essere protetti da intercettazioni, interferenze o danni. |
| 7.13 | Manutenzione delle apparecchiature | Le apparecchiature devono essere mantenute correttamente per garantire la disponibilità, l'integrità e la riservatezza delle informazioni. |
| 7.14 | Smaltimento o riutilizzo sicuro delle apparecchiature | Gli elementi delle apparecchiature contenenti supporti di memorizzazione devono essere verificati per garantire che tutti i dati sensibili e il software concesso in licenza siano stati rimossi o sovrascritti in modo sicuro prima dello smaltimento o del riutilizzo. |
| **8** | **Controlli tecnologici** | |
| 8.1 | Dispositivi endpoint utente | Le informazioni archiviate, elaborate o accessibili tramite i dispositivi endpoint degli utenti devono essere protette. |
| 8.2 | Diritti di accesso privilegiati | L'assegnazione e l'uso dei diritti di accesso privilegiato dovrebbero essere limitati e gestiti. |
| 8.3 | Limitazione dell'accesso alle informazioni | L'accesso alle informazioni e ad altre risorse associate dovrebbe essere limitato in conformità con la politica specifica per argomento stabilita sul controllo dell'accesso. |
| 8.4 | Accesso al codice sorgente | L'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software deve essere gestito in modo appropriato. |
| 8.5 | Autenticazione sicura | Le tecnologie e le procedure di autenticazione sicura dovrebbero essere implementate in base alle restrizioni di accesso alle informazioni e alla politica specifica per argomento sul controllo dell'accesso. |
| 8.6 | Gestione della capacità | L'uso delle risorse dovrebbe essere monitorato e adeguato in linea con i requisiti di capacità attuali e previsti. |
| 8.7 | Protezione contro i malware | La protezione contro il malware dovrebbe essere implementata e supportata da un'adeguata consapevolezza degli utenti. |
| 8.8 | Gestione delle vulnerabilità tecniche | È necessario ottenere informazioni sulle vulnerabilità tecniche dei sistemi informativi in uso, valutare l'esposizione dell'organizzazione a tali vulnerabilità e adottare misure appropriate. |
| 8.9 | Gestione della configurazione | Le configurazioni, comprese le configurazioni di sicurezza, di hardware, software, servizi e reti dovrebbero essere stabilite, documentate, implementate, monitorate e riviste. |
| 8.10 | Cancellazione delle informazioni | Le informazioni memorizzate nei sistemi informatici, nei dispositivi o in qualsiasi altro supporto di memorizzazione devono essere cancellate quando non sono più necessarie. |
| 8.11 | Mascheramento dei dati | Il mascheramento dei dati deve essere utilizzato in conformità con la politica specifica dell'argomento dell'organizzazione sul controllo degli accessi e altre politiche relative all'argomento specifico e i requisiti aziendali, tenendo in considerazione la legislazione applicabile. |
| 8.12 | Prevenzione della fuga di dati | Le misure di prevenzione della fuga di dati dovrebbero essere applicate a sistemi, reti e qualsiasi altro dispositivo che elabora, archivia o trasmette informazioni sensibili. |
| 8.13 | Backup delle informazioni | Le copie di backup di informazioni, software e sistemi devono essere conservate e testate regolarmente in conformità con la politica concordata specifica per argomento sul backup. |
| 8.14 | Ridondanza delle strutture di elaborazione delle informazioni | Le strutture di elaborazione delle informazioni dovrebbero essere implementate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità. |
| 8.15 | Registrazione | I registri che registrano attività, eccezioni, guasti e altri eventi rilevanti dovrebbero essere prodotti, archiviati, protetti e analizzati. |
| 8.16 | Attività di monitoraggio | Reti, sistemi e applicazioni dovrebbero essere monitorati per comportamenti anomali e azioni appropriate intraprese per valutare potenziali incidenti di sicurezza delle informazioni. |
| 8.17 | Sincronizzazione dell'orologio | Gli orologi dei sistemi di elaborazione delle informazioni utilizzati dall'organizzazione dovrebbero essere sincronizzati con fonti di tempo approvate. |
| 8.18 | Utilizzo di programmi di utilità privilegiati | L'uso di programmi di utilità che possono essere in grado di ignorare i controlli del sistema e delle applicazioni dovrebbe essere limitato e strettamente controllato. |
| 8.19 | Installazione di software su sistemi operativi | Dovrebbero essere implementate procedure e misure per gestire in modo sicuro l'installazione del software sui sistemi operativi. |
| 8.20 | Sicurezza delle reti | Le reti e i dispositivi di rete devono essere protetti, gestiti e controllati per proteggere le informazioni nei sistemi e nelle applicazioni. |
| 8.21 | Sicurezza dei servizi di rete | I meccanismi di sicurezza, i livelli di servizio dei requisiti di servizio dei servizi di rete dovrebbero essere identificati, implementati e monitorati. |
| 8.22 | Segregazione delle reti | I gruppi di servizi informativi, utenti e sistemi informativi dovrebbero essere segregati nelle reti dell'organizzazione. |
| 8.23 | Filtraggio Web | L'accesso a siti Web esterni deve essere gestito per ridurre l'esposizione a contenuti dannosi. |
| 8.24 | Uso della crittografia | Dovrebbero essere definite e attuate regole per l'uso efficace della crittografia, inclusa la gestione delle chiavi crittografiche. |
| 8.25 | Ciclo di vita dello sviluppo sicuro | Dovrebbero essere stabilite e applicate regole per lo sviluppo sicuro di software e sistemi. |
| 8.26 | Requisiti di sicurezza dell'applicazione | I requisiti di sicurezza delle informazioni devono essere identificati, specificati e approvati durante lo sviluppo o l'acquisizione di applicazioni. |
| 8.27 | Architettura di sistema sicura e principi ingegneristici | I principi per la progettazione di sistemi sicuri dovrebbero essere stabiliti, documentati, mantenuti e applicati a qualsiasi attività di sviluppo del sistema informativo. |
| 8.28 | Codifica sicura | I principi di codifica sicura dovrebbero essere applicati allo sviluppo del software. |
| 8.29 | Test di sicurezza in fase di sviluppo e accettazione | I processi di test di sicurezza dovrebbero essere definiti e implementati nel ciclo di vita dello sviluppo. |
| 8.30 | Sviluppo in outsourcing | L'organizzazione dovrebbe dirigere, monitorare e rivedere le attività relative allo sviluppo del sistema in outsourcing. |
| 8.31 | Separazione degli ambienti di sviluppo, test e produzione | Gli ambienti di sviluppo, test e produzione dovrebbero essere separati e protetti. |
| 8.32 | Gestione del cambiamento | Le modifiche alle strutture di elaborazione delle informazioni e ai sistemi informativi dovrebbero essere soggette a procedure di gestione delle modifiche. |
| 8.33 | Informazioni sul test | Le informazioni sui test dovrebbero essere opportunamente selezionate, protette e gestite. |
| 8.34 | Protezione dei sistemi informativi durante i test di audit | I test di audit e altre attività di assicurazione che coinvolgono la valutazione dei sistemi operativi dovrebbero essere pianificati e concordati tra il collaudatore e la direzione appropriata. |