|  |  |
| --- | --- |
| EVIDENZE DA FORNIRE | ESEMPI |
| A.6 RISK ASSESSMENT, CLASSIFICAZIONE DELLE INFORMAZIONI E SOA (Statement Of Applicability) | RISK ASSESSMENT  Una procedura di analisi dei rischi e un documento in cui sia presente l’analisi dei rischi della sicurezza delle informazioni.  CLASSIFICAZIONE DELLE INFORMAZIONI  Occorre fare un elenco delle informazioni da proteggere in termini di RISERVATEZZA, DISPONIBILITÀ, INTEGRITÀ.  In genere, la cosa più semplice è creare un file Excel con alcune colonne [informazione] es. dati di sorveglianza sanitaria, dati dei fornitori, dati dei clienti, dati dei registri della formazione, dati amministrativi, buste paga  *Formato*: elettronico o cartaceo  *Asset in cui si trova l’informazione*: es. computer, cloud, armadietto  *Owner dell’asset*: il responsabile della sicurezza dell’asset  *Classificazione dell’informazione*: in genere si sceglie la seguente scala   * *Pubblico*: possono essere lette all’esterno * *Interno*: possono circolare solo all’interno dell’organizzazione * *Riservato*: solo alcune persone all’interno dell’azienda possono accedere * *Classificato*: solo la direzione può accedervi   *Esempi di documenti riservati*:   * Bozza di un bilancio di una SpA, prima che venga pubblicato * Architettura di rete * Risultati delle Vulnerability Assessment * Dati personali dei dipendenti * Dati della sorveglianza sanitaria * Dati delle buste paga dei dipendenti   *Esempi di dati ad uso interno*:   * Elaborati di progetto * Preventivi * Dati di fatturazione * Procedure di sistema   La scelta della classificazione è dovuta sostanzialmente al rischio che si corre se i dati perdono di riservatezza e/o integrità e/o disponibilità.  SOA  Un elenco dei controlli dell’Annex 27001, con la motivazione delle eventuali esclusioni. |
| A.7 SICUREZZA DELLE RISORSE UMANE | Evidenze di formazione che attestino la competenza degli amministratori di sistema al ruolo che ricoprono prassi ed evidenze di controlli per la verifica del background effettuati su tutti i candidati all'impiego in accordo con le leggi, con i regolamenti pertinenti e con l’etica.  Anche nel caso in cui gli amministratori di sistema siano esterni all’azienda occorre fornire evidenze di incarico, formazione e accordi di riservatezza.  Esempi:   1. organigramma di ciascuna sede (amministratori di sistema, ecc.) 2. nomine amministratori di sistema (verbale di nomina) 3. processo di *onboarding* e *offboarding* dei dipendenti (assegnazione delle credenziali per accesso ai pc, ai sistemi, alle VPN, ecc.) con esempi documentati (e-mail, screen shot) 4. clausole di riservatezza sottoscritte dai dipendenti all’assunzione e in *onboarding* 5. evidenze di formazione dei dipendenti su qualunque tema IT e soprattutto sui temi di sicurezza informatica) |
| A.8 GESTIONE DEGLI ASSET | * Descrizione dettagliata dell’infrastruttura informatica utilizzata * Censimento dispositivi contenenti le informazioni da proteggere * Elenco licenze dei software * Procedura/policy di sicurezza e gestione degli asset |
| A.9 CONTROLLO DEGLI ACCESSI | Descrizione:   * come si accede ai sistemi digitali, lunghezza e composizione delle password, chi assegna le utenze e chi le disabilita * come vengono dismessi i dispositivi informatici obsoleti, guasti * eventuali servizi esposti su internet e il tipo di protezioni |
| A.10 CRITTOGRAFIA | * Esiste la VPN? Chi la usa e per accedere a cosa? * Le app utilizzano la crittografia *end to end*? * È in uso una *bitlocker*? Dove? |
| A.11 SICUREZZA FISICA E AMBIENTALE | Descrivere:   * se ci sono allarmi fisici all’interno della struttura, porte blindate, come è protetta la sala CED, chi ha accesso * come sono protetti i dispositivi incustoditi (screen saver con password, ecc.) * se sono presenti black list di siti internet * se viene disabilitato l’uso delle chiavette usb * se c’è l’antivirus su ogni macchina (nome antivirus) * se c’è *firewall* (nome firewall) * se è stato suddiviso l’accesso al server mediante utenti divisi per gruppi e mediante privilegi (es. *active directory*) |
| A.12 SICUREZZA DELLE OPERAZIONI | * Nome dell’antivirus * Nome del firewall * Vulnerability Assesment |
| A.13 SICUREZZA DELLE COMUNICAZIONI | * Se il server è accessibile da remoto occorre capire come è protetta questa connessione * Se il server ha dei servizi esposti su internet occorre capire come vengono protetti. |
| A.14 ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEL SISTEMA | L’azienda sviluppa/non sviluppa software |
| A.15 RAPPORTO CON I FORNITORI | Esempio di Clausole di riservatezza con i fornitori, NDA  Assegnazione di utenze ai fornitori quando lavorano per noi sui nostri sistemi  Se utilizzate servizi di terze parti (Microsoft, AWS, etc reperire le certificazioni ISO 27001 che normalmente si scaricano dai siti |
| A.16 GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI | Se è stato fatto un Vulnerability Assessment (VA) e sono emerse delle vulnerabilità, descrivere:   * evidenze delle vulnerabilità * modalità di mitigazione |
| A.17 ASPETTI DI SICUREZZA DELLE INFORMAZIONI DELLA GESTIONE DELLA CONTINUITÀ OPERATIVA | Occorre redigere una procedura che descrive per ciascuno dei seguenti eventi cosa fare per ripristinare la continuità operativa:   * guasto elettrico * guasto del server * caduta della connettività internet * incendio |
| A.18 GESTIONE DI COMMESSE A COPERTURA DI SCOPO | Per ciascuna commessa a cui si sta lavorando:   * descrivere l’oggetto e il cliente * fare un elenco dei file prodotti per la commessa (da proteggere) * annotare chi sta lavorando alla commessa, con quali strumenti software, hardware e cloud |