ISO/IEC 27001:2022 + Amd 1:2024 Sistemi di gestione della sicurezza delle informazioni (SGSI)

Sicurezza delle informazioni, SGSI, certificabile a livello mondiale

181 requisiti. Questa norma è certificabile da un organismo accreditato. Versione di 07/2026.

La norma ISO/IEC 27001 stabilisce i requisiti per un sistema di gestione della sicurezza delle informazioni: basato sul rischio, documentato e con efficacia dimostrabile. Una valutazione secondo questa norma è un audit di certificazione accreditato in due fasi (esame documentale, poi verifica dell'efficacia in loco), seguito da audit di sorveglianza annuali e dalla ricertificazione dopo tre anni.

Azienda	Data	Redatto da

4 Contesto dell'organizzazione 8

4.1-1 Le questioni esterne e interne che influiscono sulla capacità dell'organizzazione di conseguire i risultati attesi del SGSI sono individuate e mantenute aggiornate.

Come si dimostra: Si dimostra tramite un'analisi del contesto, sia come documento a sé stante sia come sezione del manuale del SGSI: contesto di mercato, situazione di clienti e contratti, quadro normativo (RGPD, NIS2), stack tecnologico, organico, dipendenza dai fornitori cloud. Per le organizzazioni piccole basta una tabella di una pagina con data e ciclo di revisione, a condizione che il riesame della direzione dimostri un aggiornamento effettivo.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

4.1-2 L'organizzazione ha determinato se il cambiamento climatico è una questione rilevante per essa. La determinazione è motivata, indipendentemente dal fatto che la risposta sia affermativa o negativa.

Come si dimostra: Questo requisito è stato introdotto dall'Amd 1:2024 e gli auditor lo chiedono in modo specifico. Mantenere una riga dedicata nell'analisi del contesto: ondate di calore che influiscono sulle sale server e sulla disponibilità, fenomeni meteorologici estremi che colpiscono i data center dei fornitori cloud, stabilità della rete elettrica. Un risultato motivato di non rilevante è accettabile, una voce mancante no.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

4.2-1 Sono individuate le parti interessate rilevanti per il SGSI.

Come si dimostra: Elenco delle parti interessate che copre clienti, personale, responsabili e subresponsabili del trattamento, autorità di vigilanza, assicuratori, l'organismo di certificazione e gli azionisti. Nelle organizzazioni piccole basta una tabella con parte interessata, aspettativa e fonte dell'aspettativa.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

4.2-2 Sono individuati i requisiti rilevanti di queste parti interessate, compresi quelli relativi al cambiamento climatico.

Come si dimostra: Per ciascuna parte interessata indicare la fonte concreta: clausola contrattuale, accordo sul trattamento dei dati, questionario del cliente, obbligo di legge. L'Amd 1:2024 aggiunge una nota secondo cui le parti interessate possono avere requisiti legati al cambiamento climatico. Non è un requisito deve autonomo, ma gli auditor lo sollevano di frequente, ad esempio domande sulla sostenibilità nell'audit fornitori di un cliente importante. Basta una riga nella tabella delle parti interessate con il risultato, incluso nessuno di questo tipo.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

4.2-3 È deciso ed è tracciabile quali di questi requisiti sono affrontati tramite il SGSI.

Come si dimostra: Aggiungere una colonna alla tabella delle parti interessate che rimandi alla regola che affronta il requisito (politica, controllo, allegato contrattuale). Questo dimostra che i requisiti non sono stati soltanto raccolti, ma effettivamente elaborati.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

4.3-1 **È determinato il campo di applicazione del SGSI, tenendo conto delle questioni di cui al punto 4.1, dei requisiti di cui al punto 4.2, nonché delle interfacce e delle dipendenze con attività svolte da terzi.**

Come si dimostra: Il campo di applicazione indica sedi, unità organizzative, prodotti, sistemi e confini di rete. Le parti esternalizzate (hosting, fornitori di pagamento, supporto) sono descritte come interfacce con un confine di responsabilità chiaro. Un campo di applicazione artificiosamente ristretto che escluda processi centrali viene respinto dagli organismi di certificazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

4.3-2 **Il campo di applicazione è disponibile come informazione documentata e indica in modo univoco i confini del SGSI.** Documento

Come si dimostra: Un documento di campo di applicazione approvato con versione, data e avallo dell'alta direzione. La sua formulazione esatta comparirà poi sul certificato, quindi va redatto con precisione e in modo citabile pubblicamente.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

4.4-1 **Il SGSI, compresi i processi necessari e le loro interazioni, è stabilito, attuato, mantenuto e migliorato con continuità.**

Come si dimostra: Una mappa dei processi o un elenco di processi che colleghi la gestione del rischio, la gestione degli incidenti, la gestione dei cambiamenti, l'audit e il riesame della direzione con responsabili e frequenza. L'evidenza viva conta più dello schema: ticket, verbali, appuntamenti a calendario.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5 Leadership 8

5.1-1 **L'alta direzione si assume la responsabilità dell'efficacia del SGSI e garantisce che la politica e gli obiettivi siano stabiliti e compatibili con l'orientamento strategico.**

Come si dimostra: L'evidenza comprende approvazioni firmate della politica, del campo di applicazione e della Dichiarazione di Applicabilità, verbali del riesame della direzione e decisioni di budget documentate. Nelle organizzazioni molto piccole l'alta direzione coincide spesso con il responsabile del SGSI, il che è accettabile ma deve essere dichiarato apertamente nella definizione del ruolo.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.1-2 **I requisiti del SGSI sono integrati nei processi aziendali e viene comunicata l'importanza di una sicurezza delle informazioni efficace.**

Come si dimostra: Si dimostra al meglio quando la sicurezza non è un raccoglitore a parte: un criterio di sicurezza nella definizione di fatto, un controllo di sicurezza nel processo commerciale o di acquisto, un punto ricorrente sulla sicurezza nei verbali delle riunioni di team.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.1-3 **La direzione fornisce le risorse necessarie, sostiene le persone che contribuiscono all'efficacia del SGSI e promuove il miglioramento continuo.**

Come si dimostra: Budget di sicurezza approvato, tempo assegnato alla formazione, incarico ad auditor esterni o a professionisti di penetration test. Un registro di miglioramenti o azioni con voci distribuite su più trimestri dimostra continuità e non uno sforzo occasionale.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.2-1 **È stabilita una politica di sicurezza delle informazioni appropriata allo scopo dell'organizzazione, che fornisce un quadro di riferimento per gli obiettivi di sicurezza delle informazioni.** Documento

Come si dimostra: Un documento di politica breve e approvato, due o tre pagine sono sufficienti. Indica gli obiettivi di protezione, il campo di applicazione, le responsabilità e il principio dell'approccio basato sul rischio. Un testo generico da modello senza collegamento al business reale risalta negativamente in audit.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.2-2 **La politica include un impegno a soddisfare i requisiti applicabili e un impegno al miglioramento continuo del SGSI.** Documento

Come si dimostra: Entrambi gli impegni devono comparire come frasi esplicite nella politica e vengono letti parola per parola nell'audit di fase 1. Inoltre, rimandare ai processi sottostanti (registro legale, registro dei miglioramenti).

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.2-3 **La politica è comunicata all'interno dell'organizzazione ed è disponibile per le parti interessate, ove opportuno.** Documento

Come si dimostra: Evidenza tramite una voce su intranet o wiki con obbligo di lettura, una checklist di onboarding con conferma, oppure un riepilogo pubblicato sul sito web. Una lista di distribuzione con ricevute di conferma è la prova solida più semplice.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.3-1 **Le responsabilità e le autorità per i ruoli rilevanti ai fini della sicurezza sono assegnate e comunicate all'interno dell'organizzazione.**

Come si dimostra: Una matrice dei ruoli (RACI) che copra il responsabile del SGSI, i responsabili del rischio, i responsabili degli asset, il coordinatore degli incidenti e il referente per la protezione dei dati. Nei team unipersonali o molto piccoli, assegnare ogni ruolo a una persona nominata e documentare apertamente il conseguente cumulo di ruoli invece di occultarlo.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

5.3-2 **L'autorità per garantire che il SGSI sia conforme alla norma e per riferire sulle prestazioni del SGSI all'alta direzione è assegnata a un ruolo.**

Come si dimostra: Una lettera di nomina o una descrizione di ruolo per il responsabile del SGSI con una linea di reporting esplicita verso la direzione. La linea di reporting deve essere effettivamente comprovata dai verbali del riesame della direzione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6 Pianificazione 21

6.1.1-1 **Partendo dalle questioni di cui al punto 4.1 e dai requisiti di cui al punto 4.2, sono individuati i rischi e le opportunità da affrontare, affinché il SGSI consegua i risultati attesi e siano prevenuti gli effetti indesiderati.**

Come si dimostra: Un registro che colleghi le questioni di contesto a rischi e opportunità, tenuto separatamente oppure all'interno del registro dei rischi. Ciò che conta è la tracciabilità: ogni questione dell'analisi del contesto deve condurre in modo visibile a una valutazione o a una decisione motivata di non considerarla.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.1-2 **Sono pianificate le azioni per affrontare questi rischi e opportunità, integrate nei processi del SGSI, e ne viene valutata l'efficacia.**

Come si dimostra: Piano d'azione con responsabile, scadenza e criterio di efficacia. Mantenere la valutazione dell'efficacia come colonna a sé stante, altrimenti nell'audit mancherà la prova che l'azione non solo è stata attuata, ma anche verificata.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.2-1 **È definito e applicato un processo di valutazione del rischio per la sicurezza delle informazioni, che include i criteri di accettazione del rischio e i criteri per condurre le valutazioni del rischio.** Documento

Come si dimostra: Una politica di gestione del rischio con scale di probabilità e impatto, una matrice del rischio definita e una soglia di accettazione chiara. La soglia deve essere un numero o una zona, non una frase come a nostra discrezione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.2-2 **Il processo garantisce che valutazioni del rischio ripetute producano risultati coerenti, validi e comparabili.**

Come si dimostra: Si dimostra tramite una metodologia fissa con scale definite e confrontando due versioni della valutazione: stessi rischi, stessa logica di valutazione, differenze spiegabili. Una versione datata del registro dei rischi dell'anno precedente è l'evidenza più solida in questo punto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.2-3 **I rischi per la sicurezza delle informazioni sono individuati per rilevare la perdita di riservatezza, integrità e disponibilità all'interno del campo di applicazione, e a ogni rischio è assegnato un responsabile del rischio.**

Come si dimostra: Registro dei rischi che fa riferimento ad asset o processi, ai tre obiettivi di protezione e a un responsabile del rischio nominato. Il responsabile del rischio deve avere l'autorità di accettarlo; nelle organizzazioni piccole si tratta di norma dell'amministratore.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.2-4 **I rischi individuati sono analizzati: sono determinate le potenziali conseguenze, la probabilità realistica e il livello di rischio risultante.**

Come si dimostra: Colonne per impatto, probabilità e livello di rischio risultante, ciascuna con una breve motivazione. Una frase di motivazione per rischio evita il rilievo di audit più frequente, ossia numeri senza derivazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.2-5 **I rischi sono confrontati con i criteri di accettazione e sono prioritizzati per il trattamento.**

Come si dimostra: Il registro dei rischi deve mostrare quali rischi superano la soglia di accettazione e in quale ordine saranno trattati. Basta una vista ordinata o una colonna di priorità.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.2-6 **Il processo di valutazione del rischio è disponibile come informazione documentata.** Documento

Come si dimostra: La metodologia stessa è un documento obbligatorio, non solo il suo risultato. Una politica approvata con versione e data di approvazione, collegata dall'indice dei documenti del SGSI.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.3-1 **Per ogni rischio che supera la soglia di accettazione è selezionata un'opzione di trattamento adeguata (ridurre, evitare, trasferire o accettare).**

Come si dimostra: Una colonna con l'opzione di trattamento nel registro dei rischi. Quando un rischio è accettato, registrare la motivazione e l'approvazione formale del responsabile del rischio; quando è trasferito, indicare il contratto o la polizza assicurativa.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.3-2 **Sono determinati tutti i controlli necessari per attuare le opzioni di trattamento del rischio scelte.**

Come si dimostra: Formulare i controlli in modo concreto e verificabile, con responsabile e scadenza. È valido rimandare a lavori tecnici già in corso (implementazione MFA, test di backup), purché rimandino a un ticket o a un artefatto di configurazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.3-3 **I controlli determinati sono confrontati con i controlli dell'allegato A per verificare che nessun controllo necessario sia stato trascurato.**

Come si dimostra: Il confronto è un passaggio autonomo e tracciabile, non un sottoprodotto. Si evidenzia tramite una colonna di corrispondenza nel registro dei rischi che rimanda ai numeri dell'allegato A, insieme a un verbale datato del confronto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.3-4 **Esiste una Dichiarazione di Applicabilità (SoA). Valuta individualmente tutti i 93 controlli dell'allegato A, indica l'applicabilità con motivazione per ciascun controllo, lo stato di attuazione e la motivazione per ogni esclusione.** Documento

Come si dimostra: La Dichiarazione di Applicabilità è il documento obbligatorio centrale e la mappa dell'intero audit. Deve essere completa: anche i controlli non applicabili compaiono con una motivazione, mai come riga vuota. Colonne consigliate: numero del controllo, titolo, applicabile sì o no, motivazione, stato di attuazione, riferimento alla politica o all'evidenza, collegamento al rischio. Versione e approvazione della direzione sono obbligatorie, perché la Dichiarazione di Applicabilità viene confrontata con la realtà a ogni audit di sorveglianza.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.3-5 **È elaborato un piano di trattamento del rischio che riunisce controlli, responsabilità, scadenze e risorse necessarie.** Documento

Come si dimostra: Può essere una scheda nel foglio di calcolo dei rischi o una bacheca di progetto. Ciò che conta è che le scadenze siano realistiche e che i termini non rispettati siano stati visibilmente ripianificati, perché è esattamente quello che verifica l'auditor.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.3-6 **Il piano di trattamento del rischio è approvato dai responsabili del rischio e i rischi residui rimanenti sono da questi formalmente accettati.** Documento

Come si dimostra: Firma, approvazione elettronica o una decisione datata a verbale. Basta una riga nel verbale del riesame della direzione che rimandi alla versione del registro, purché la versione sia univoca.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.1.3-7 **Il processo di trattamento del rischio è disponibile come informazione documentata.** Documento

Come si dimostra: Di norma coperto nello stesso documento di politica della valutazione del rischio. Deve essere descritto il flusso dalla valutazione, attraverso la selezione delle opzioni, fino all'accettazione del rischio residuo.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.2-1 **Sono stabiliti obiettivi di sicurezza delle informazioni per le funzioni e i livelli pertinenti, coerenti con la politica e, ove possibile, misurabili.**

Come si dimostra: Una scheda obiettivi con tre o sei obiettivi, ciascuno con un indicatore, un valore di partenza, un valore obiettivo e una scadenza. Esempio: quota di sistemi con MFA portata dall'80 al 100 per cento entro la fine del trimestre. Gli obiettivi senza un numero non contano come misurabili.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.2-2 **Gli obiettivi tengono conto dei requisiti di sicurezza delle informazioni applicabili nonché dei risultati della valutazione e del trattamento del rischio.**

Come si dimostra: Aggiungere una colonna di origine alla scheda obiettivi: da quale rischio, quale requisito del cliente o quale obbligo di legge deriva l'obiettivo. Questo evita obiettivi che sembrino arbitrari.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.2-3 **Gli obiettivi sono monitorati, comunicati e aggiornati secondo necessità.**

Come si dimostra: Monitoraggio trimestrale dell'avanzamento nella scheda obiettivi, più la comunicazione al team, ad esempio una breve nota sul wiki o un punto all'ordine del giorno della riunione di team. Le versioni storiche dimostrano che gli aggiornamenti avvengono davvero.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.2-4 **Gli obiettivi di sicurezza delle informazioni sono disponibili come informazione documentata.** Documento

Come si dimostra: Basta un documento di obiettivi approvato e datato. Può far parte del riesame della direzione, ma deve esistere lì come sezione propria e recuperabile.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.2-5 **Per ciascun obiettivo è pianificato cosa sarà fatto, quali risorse sono necessarie, chi è responsabile, quando sarà completato e come saranno valutati i risultati.**

Come si dimostra: Questi cinque punti sono verificabili singolarmente e vengono chiesti singolarmente in audit. Impostarli come cinque colonne nella scheda obiettivi, così la conformità è visibile a colpo d'occhio.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

6.3-1 **Laddove l'organizzazione determini che sono necessari cambiamenti al SGSI, tali cambiamenti sono realizzati in modo pianificato.**

Come si dimostra: Si evidenzia tramite richieste di cambiamento, verbali o ticket che mostrino l'evento scatenante, la valutazione d'impatto, l'approvazione e l'attuazione. Eventi scatenanti tipici nelle organizzazioni piccole: cambio di fornitore cloud, nuove sedi, la prima assunzione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7 Supporto 15

7.1-1 **Sono individuate e fornite le risorse necessarie per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo del SGSI.**

Come si dimostra: Una voce di budget per la sicurezza, licenze di strumenti (gestore di password, MDM, piattaforma di log), giornate persona pianificate per il mantenimento del SGSI e servizi di audit esterno. Una fattura o un'approvazione di budget lo dimostrano più rapidamente di qualsiasi testo.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7.2-1 **È determinata la competenza necessaria delle persone il cui lavoro incide sulle prestazioni di sicurezza delle informazioni.**

Come si dimostra: Matrice delle competenze o profili di ruolo che elencano le conoscenze richieste per ruolo, ad esempio sviluppo sicuro per gli sviluppatori, gestione degli incidenti per il coordinatore. Nei team molto piccoli basta una riga per persona.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7.2-2 **La competenza è garantita sulla base di un'istruzione, una formazione o un'esperienza adeguate.**

Come si dimostra: Certificati, conferme di corsi, curricula o esperienza pratica documentata. L'autoapprendimento è accettabile se evidenziato, ad esempio tramite attestati di completamento di corsi online o test di conoscenza interni superati.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7.2-3 **Laddove esistano carenze di competenza, sono state intraprese azioni per colmarle e ne è stata valutata l'efficacia.**

Come si dimostra: Piano di formazione con un confronto tra previsto e realizzato e una verifica di efficacia, ad esempio un punteggio di test, un tasso di clic in una simulazione di phishing o un'osservazione sul posto di lavoro. La verifica di efficacia viene spesso dimenticata ed è un classico rilievo minore.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7.2-4 **È disponibile un'informazione documentata appropriata come evidenza della competenza.** Documento

Come si dimostra: Una cartella di competenza o formazione per persona con evidenze e date. Nelle organizzazioni piccole basta una directory con i documenti PDF salvati più una tabella riassuntiva.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7.3-1 **Le persone che lavorano nell'ambito del campo di applicazione sono consapevoli della politica di sicurezza delle informazioni.**

Come si dimostra: Conferma all'onboarding e dopo ogni modifica della politica, con data e versione. Una funzione di ricevuta di lettura sul wiki o un elenco firmato sono sufficienti.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7.3-2 **Le persone conoscono il proprio contributo all'efficacia del SGSI e i benefici del miglioramento delle prestazioni di sicurezza delle informazioni.**

Come si dimostra: Materiale formativo e liste di presenza in cui sia visibile il legame con il lavoro proprio della persona. Gli auditor intervistano direttamente il personale, quindi formare con esempi concreti e quotidiani anziché citazioni astratte della norma.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7.3-3 **Le persone conoscono le conseguenze della non conformità ai requisiti del SGSI.**

Come si dimostra: Indicare le conseguenze nelle diapositive di formazione e nelle istruzioni di lavoro e collegarle al processo di cui al punto A.6.4. Anche le organizzazioni senza dipendenti devono coprire questo aspetto per contrattisti e liberi professionisti tramite i loro contratti.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7.4-1 **È determinata la comunicazione interna ed esterna rilevante per il SGSI: cosa viene comunicato, quando, con chi e con quali mezzi.**

Come si dimostra: Una matrice di comunicazione con righe come incidente di sicurezza ai clienti, notifica all'autorità di vigilanza entro 72 ore, rapporto di stato mensile alla direzione. È la base della comunicazione di crisi e viene rivista dopo ogni incidente.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

7.5.1-1 **Il SGSI include l'informazione documentata richiesta dalla norma, nonché l'informazione documentata che l'organizzazione ha determinato essere necessaria per l'efficacia del SGSI.** Documento

Come si dimostra: Un indice dei documenti che elenchi ogni documento del SGSI con scopo, responsabile, versione e ubicazione di archiviazione. Dimostra che i documenti obbligatori sono completi ed è il punto di accesso più rapido per l'auditor.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7.5.2-1 **Nella creazione e nell'aggiornamento dei documenti sono garantiti un'identificazione, un formato e un supporto appropriati, e i documenti sono riesaminati e approvati per idoneità.**

Come si dimostra: Un'intestazione di documento uniforme con titolo, versione, data, autore e approvatore. Negli ambienti basati su Git, i riesami delle pull request con approvazione soddisfano il requisito di riesame e approvazione, purché la cronologia sia immutabile.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7.5.3-1 **L'informazione documentata è disponibile e idonea all'uso dove e quando è necessaria.**

Come si dimostra: Un'ubicazione di archiviazione centrale raggiungibile da tutti gli aventi diritto, con funzione di ricerca. Verificabile a campione: una qualsiasi istruzione di lavoro deve poter essere trovata in meno di un minuto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7.5.3-2 **L'informazione documentata è adeguatamente protetta, in particolare contro la perdita di riservatezza, l'uso improprio e la perdita di integrità.**

Come si dimostra: Diritti di accesso basati sui ruoli ai documenti del SGSI, versionamento con cronologia, protezione in scrittura per le versioni approvate e un backup del repository documentale. L'evidenza del backup è la parte più spesso dimenticata.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7.5.3-3 **Sono disciplinati la distribuzione, l'accesso, il recupero, l'archiviazione, il controllo delle modifiche, nonché la conservazione e la disposizione dell'informazione documentata.**

Come si dimostra: Una breve regola di controllo documentale con termini di conservazione e regole di cancellazione. Deve essere riconciliata con gli obblighi di legge (diritto commerciale, diritto tributario, RGPD) ed è la base per i punti A.5.33 e A.8.10.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

7.5.3-4 **L'informazione documentata di origine esterna necessaria per pianificare e far funzionare il SGSI è identificata e controllata.**

Come si dimostra: Un elenco di documenti esterni con versione e fonte: norme, testi di legge, guide di hardening dei fornitori, documentazione di sicurezza cloud, accordi sul trattamento dei dati. Senza un riferimento di versione il controllo non può essere dimostrato.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

8 Attività operative 8

8.1-1 **Sono pianificati, attuati e controllati i processi necessari per soddisfare i requisiti di sicurezza delle informazioni e per attuare le azioni di cui al punto 6, e sono stabiliti criteri per tali processi.**

Come si dimostra: Un manuale operativo o runbook con criteri chiari, ad esempio il tempo massimo per distribuire le patch critiche, criteri di rilascio per i deployment, soglie di allerta. I criteri senza numeri non hanno alcun valore in audit.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

8.1-2 **È disponibile l'informazione documentata nella misura necessaria per avere fiducia che i processi siano stati eseguiti come pianificato.** Documento

Come si dimostra: Registrazioni operative come evidenza: storico dei ticket, esecuzioni della pipeline CI, rapporti sulle patch, log dei backup, riesami degli accessi. Queste registrazioni sono la prova reale di efficacia nell'audit di fase 2.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

8.1-3 **I cambiamenti pianificati sono controllati e sono riesaminate le conseguenze dei cambiamenti non intenzionali; ove necessario, sono mitigati gli effetti avversi.**

Come si dimostra: Un processo di gestione dei cambiamenti con approvazione e un percorso di rollback, collegato al punto A.8.32. Per i cambiamenti non intenzionali (configurazione errata, escalation accidentale di privilegi) documentare l'incidente ed evidenziare la correzione.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

8.1-4 **Sono individuati e controllati i processi, i prodotti e i servizi forniti esternamente rilevanti per il SGSI.**

Come si dimostra: Un elenco fornitori con criticità, riferimento contrattuale e stato dell'evidenza (il certificato ISO 27001 del fornitore, il rapporto SOC 2, l'accordo sul trattamento dei dati). Per le organizzazioni piccole è la leva più importante, perché la maggior parte dell'IT gira comunque all'esterno.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

8.2-1 **Le valutazioni del rischio sono condotte a intervalli pianificati e ogni volta che si verificano cambiamenti o incidenti significativi, tenendo conto dei criteri stabiliti.**

Come si dimostra: Un ritmo (tipicamente annuale) più eventi scatenanti definiti per valutazioni non programmate. Si evidenzia tramite versioni datate del registro dei rischi e voci nel calendario o nel sistema di ticket.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

8.2-2 **I risultati delle valutazioni del rischio sono conservati come informazione documentata.** Documento

Come si dimostra: Versioni storiche del registro dei rischi con date, non solo lo stato attuale. Sovrascrivere il file rende impossibile dimostrare l'evoluzione; il versionamento nel file system o in Git risolve questo problema.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

8.3-1 **Il piano di trattamento del rischio è attuato.**

Come si dimostra: Confrontare il piano con la realtà: azioni completate con data di attuazione e un artefatto concreto (configurazione, politica, contratto). Le azioni aperte necessitano di una motivazione documentata e di una nuova scadenza.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

8.3-2 **I risultati del trattamento del rischio sono conservati come informazione documentata.** Documento

Come si dimostra: Rapporti di stato o azioni chiuse con un riferimento all'evidenza. Basta il registro stesso se ogni riga riporta una data di completamento e un collegamento all'evidenza.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

9 Valutazione delle prestazioni 21

9.1-1 **È determinato cosa deve essere monitorato e misurato, compresi i processi e i controlli di sicurezza delle informazioni.**

Come si dimostra: Una scheda indicatori con un numero gestibile di misure solide: arretrato delle patch, copertura MFA, tempo di risoluzione degli incidenti, esito dell'ultimo test di ripristino, rilievi aperti. Pochi indicatori effettivamente raccolti valgono più di una lunga lista di desideri.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.1-2 **Sono definiti i metodi di monitoraggio, misurazione, analisi e valutazione, e producono risultati validi.**

Come si dimostra: Documentare la fonte dei dati e il calcolo per ciascun indicatore, ad esempio un'esportazione dallo scanner delle vulnerabilità o dal rapporto del provider di identità. La tracciabilità della fonte è il nucleo della validità.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.1-3 **È definito quando e da chi sono effettuati il monitoraggio e la misurazione, e quando i risultati sono analizzati e valutati.**

Come si dimostra: Aggiungere colonne di frequenza e responsabile alla scheda indicatori. Un appuntamento ricorrente a calendario per la valutazione dimostra la regolarità meglio di qualsiasi descrizione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.1-4 **I risultati del monitoraggio e della misurazione sono conservati come informazione documentata.** Documento

Come si dimostra: Valutazioni archiviate, dashboard esportate o una scheda indicatori mantenuta come serie storica. Una vista in tempo reale senza storico non soddisfa il requisito.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.1-5 **Le prestazioni di sicurezza delle informazioni e l'efficacia del SGSI sono valutate sulla base dei risultati della misurazione.**

Come si dimostra: Una valutazione scritta, non solo cifre: tendenza, cause, necessità di intervento. Questo testo di valutazione è al tempo stesso un input per il riesame della direzione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.2.1-1 **Sono condotti audit interni a intervalli pianificati che forniscono informazioni sul fatto che il SGSI sia conforme ai requisiti propri dell'organizzazione e a quelli della norma, e sia attuato efficacemente.**

Come si dimostra: Prima dell'audit di certificazione deve essere completato almeno un ciclo completo di audit interno che copra l'intero campo di applicazione. Senza di esso la certificazione è irraggiungibile; questo è uno degli ostacoli più comuni nelle prime certificazioni.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.2.2-1 **È pianificato, stabilito e mantenuto un programma di audit, che definisce frequenza, metodi, responsabilità, requisiti di pianificazione e reporting, e tiene conto dell'importanza dei processi coinvolti e dei risultati degli audit precedenti.**

Come si dimostra: Un programma di audit pluriennale che copra tutti i punti e tutti i controlli applicabili nell'arco del ciclo di certificazione, con frequenza maggiore per le aree critiche. Una semplice tabella su tre anni è del tutto sufficiente.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.2.2-2 **Per ogni audit sono definiti i criteri e il campo di applicazione dell'audit.**

Come si dimostra: Un piano di audit per ciascuna data con i criteri (la norma, le politiche interne, i contratti) e un campo di applicazione chiaro. Un piano di audit di una pagina per audit è sufficiente e funge anche da base per il rapporto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.2.2-3 **Gli auditor sono selezionati e gli audit sono condotti in modo da garantire l'obiettività e l'imparzialità. Nessuno effettua l'audit del proprio lavoro.**

Come si dimostra: L'indipendenza è l'ostacolo più severo in questo punto: chi ha redatto le politiche e configurato i sistemi non può farne l'audit. Nelle organizzazioni molto piccole questo comporta quasi sempre un auditor interno esterno, ad esempio un consulente incaricato o un collega di un'azienda partner; un contratto di audit più la dichiarazione di indipendenza dell'auditor costituiscono l'evidenza. Solo nei team sufficientemente grandi il ruolo può essere ruotato internamente verso una persona senza responsabilità sull'area sottoposta ad audit, e ciò deve poi essere riportato nella matrice dei ruoli.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.2.2-4 **I risultati dell'audit sono riferiti alla direzione competente.**

Come si dimostra: Un rapporto di audit con rilievi, non conformità, raccomandazioni e una lista di distribuzione, più l'evidenza della trasmissione alla direzione, ad esempio un punto a verbale o un'email datata di trasmissione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.2.2-5 **È conservata l'informazione documentata sul programma di audit e sui risultati dell'audit.** Documento

Come si dimostra: Conservare in un unico luogo il programma di audit, i piani di audit, i rapporti di audit e le azioni risultanti. Il collegamento tra un rilievo e un'azione correttiva (punto 10.2) deve essere visibile dall'inizio alla fine.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.1-1 **L'alta direzione riesamina il SGSI a intervalli pianificati per assicurarne la continua idoneità, adeguatezza ed efficacia.**

Come si dimostra: Almeno annualmente e programmato prima dell'audit esterno. Anche nelle organizzazioni molto piccole deve esistere un verbale datato e firmato, anche quando la direzione e il responsabile del SGSI coincidono nella stessa persona.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.2-1 **Il riesame della direzione tiene conto dello stato delle azioni derivanti da precedenti riesami della direzione.**

Come si dimostra: Il verbale inizia con una tabella di follow-up delle decisioni dell'anno precedente e del loro stato attuale. Senza questo riferimento a ritroso, il riesame è considerato incompleto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.2-2 **Il riesame della direzione tiene conto dei cambiamenti nelle questioni esterne e interne rilevanti per il SGSI, compresi gli aspetti rilevanti del cambiamento climatico.**

Come si dimostra: Un punto dedicato all'ordine del giorno che rimandi all'analisi del contesto aggiornata. Il cambiamento climatico non è nominato esplicitamente nel testo di questo punto (l'Amd 1:2024 modifica solo i punti 4.1 e 4.2), ma entra qui attraverso i cambiamenti nelle questioni del punto 4.1, e gli auditor se lo aspettano. Anche un risultato di non rilevante, invariato deve comparire nel verbale.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.2-3 **Il riesame della direzione tiene conto dei cambiamenti nelle esigenze e aspettative delle parti interessate rilevanti per il SGSI.**

Come si dimostra: Nuovi requisiti dei clienti provenienti da contratti e questionari sulla sicurezza, nuovi obblighi di legge, requisiti dell'organismo di certificazione. Registrarli come elenco con le fonti nel verbale.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.2-4 **Il riesame della direzione tiene conto del feedback sulle prestazioni di sicurezza delle informazioni, comprese le non conformità e le azioni correttive, i risultati del monitoraggio e della misurazione, i risultati degli audit e il conseguimento degli obiettivi di sicurezza delle informazioni.**

Come si dimostra: Trattare questi quattro blocchi come punti separati all'ordine del giorno, altrimenti uno di essi mancherà successivamente nel verbale. Allegare la scheda indicatori, il rapporto di audit e la scheda obiettivi come allegati.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.2-5 **Il riesame della direzione tiene conto del feedback delle parti interessate.**

Come si dimostra: Reclami dei clienti con un risvolto di sicurezza, risultati di audit dei clienti, segnalazioni dal canale di whistleblowing, feedback dei fornitori di servizi. Registrarlo nel verbale anche quando l'esito è che non ne è stato ricevuto alcuno.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.2-6 **Il riesame della direzione tiene conto dei risultati della valutazione del rischio e dello stato del piano di trattamento del rischio.**

Come si dimostra: Allegare il registro dei rischi attuale e lo stato di attuazione del piano di trattamento, con conferma esplicita dell'accettazione del rischio residuo da parte dei responsabili del rischio.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.2-7 **Il riesame della direzione tiene conto delle opportunità di miglioramento continuo.**

Come si dimostra: Un punto all'ordine del giorno con idee di miglioramento concrete e una decisione su ciascuna. Le idee accettate confluiscono nel registro dei miglioramenti come voci con scadenze.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.3-1 **I risultati del riesame della direzione includono decisioni sulle opportunità di miglioramento continuo e su qualsiasi necessità di cambiamenti al SGSI.**

Come si dimostra: Il verbale termina con una sezione decisioni: decisione, responsabile, scadenza. Un verbale senza decisioni è un rilievo in audit, perché manca allora l'effetto di leadership.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

9.3.3-2 **È conservata l'informazione documentata come evidenza dei risultati del riesame della direzione.** Documento

Come si dimostra: Verbale firmato con data, partecipanti, input, valutazione e decisioni. È uno dei primi documenti che un organismo di certificazione chiede nella fase 1.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

10 Miglioramento 7

10.1-1 **L'idoneità, l'adeguatezza e l'efficacia del SGSI sono migliorate con continuità.**

Come si dimostra: Un registro dei miglioramenti alimentato da più fonti (audit, incidenti, idee, scostamenti degli indicatori) con progresso visibile nel tempo. La continuità su più mesi è la prova, non il numero di voci.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

10.2-1 **Quando si verifica una non conformità, l'organizzazione reagisce: la controlla, la corregge e ne gestisce le conseguenze.**

Come si dimostra: Un rapporto di non conformità con un'azione immediata e una data. Le fonti sono audit interni, audit esterni, incidenti e osservazioni dell'operatività quotidiana; tutte alimentano lo stesso registro.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

10.2-2 **È valutato se sia necessaria un'azione per eliminare le cause, affinché la non conformità non si ripeta o non si verifichi altrove; ciò include la verifica dell'esistenza o del possibile verificarsi di non conformità simili.**

Come si dimostra: Documentare l'analisi delle cause radice, ad esempio con i 5 perché o il diagramma di Ishikawa, più una dichiarazione esplicita sulla trasferibilità ad altri sistemi o processi. Il passaggio sulla trasferibilità è quello più spesso omesso.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

10.2-3 **Le eventuali azioni correttive necessarie sono attuate e ne viene riesaminata l'efficacia.**

Come si dimostra: Per ciascuna azione registrare la data di attuazione, l'artefatto di evidenza e un successivo riesame di efficacia con una propria data. Due campi data per riga sono il modo più semplice per non perdere di vista il riesame di efficacia.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

10.2-4 **Ove necessario, sono apportati cambiamenti al SGSI a seguito della non conformità.**

Come si dimostra: Se una non conformità è riconducibile a una lacuna in una politica, nel registro dei rischi o nella Dichiarazione di Applicabilità, il cambiamento deve diventarvi visibile. Un riferimento dalla non conformità alla versione aggiornata del documento chiude la catena.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

10.2-5 **Le azioni correttive sono appropriate agli effetti delle non conformità riscontrate.**

Come si dimostra: Una valutazione di gravità nel registro da cui risulti la proporzionalità dell'azione. Né banalità trattate come un progetto, né deviazioni gravi affrontate con una semplice email di promemoria.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

10.2-6 **È conservata l'informazione documentata sulla natura delle non conformità, sulle azioni intraprese in risposta e sui risultati delle azioni correttive.** Documento

Come si dimostra: Un registro delle non conformità e delle azioni correttive con colonne per natura, causa, azione, responsabile, scadenza e l'esito del riesame di efficacia. È un'evidenza obbligatoria e viene richiesta a ogni audit di sorveglianza.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5 Allegato A: Controlli organizzativi 37

A.5.1 **Politiche per la sicurezza delle informazioni: sono definite una politica generale di sicurezza delle informazioni e politiche specifiche per argomento, approvate dalla direzione, comunicate e riesaminate a intervalli pianificati e ogni volta che si verificano cambiamenti significativi.** Documento

Come si dimostra: Un insieme di politiche con versione, data di approvazione e prossima data di riesame, più l'evidenza della presa visione. Per le organizzazioni piccole bastano una politica quadro e una manciata di politiche specifiche (accesso, crittografia, lavoro da remoto, incidenti).

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.2 **Ruoli e responsabilità per la sicurezza delle informazioni: i ruoli e le responsabilità in materia di sicurezza delle informazioni sono definiti e assegnati secondo le esigenze dell'organizzazione.**

Come si dimostra: Una matrice dei ruoli con nomi, sostituti e compiti. Nelle organizzazioni molto piccole indicare apertamente dove più ruoli si cumulano su una sola persona e collegare questo aspetto ai controlli compensativi di cui al punto A.5.3.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.3 **Separazione dei compiti: i compiti e le aree di responsabilità destinati a controllarsi reciprocamente non sono affidati a un'unica persona. L'obiettivo è che nessuno possa avviare, approvare e occultare un cambiamento da solo.**

Come si dimostra: Nelle organizzazioni piccole la separazione completa è strutturalmente impossibile; un'affermazione generica di conformità crolla subito nel colloquio di audit. Ciò che regge è un'analisi onesta: quali combinazioni di compiti sono critiche (sviluppare e rilasciare, concedere diritti e utilizzarli, avviare e approvare pagamenti), quali di esse ricadono su una sola persona e quali controlli compensativi si applicano. Approcci collaudati sono i log di audit immutabili accessibili a terzi, la MFA sugli account privilegiati, i gate automatizzati della CI e la protezione dei branch al posto della revisione a quattro occhi, un riesame periodico dei log da parte di una persona esterna, e l'approvazione separata dei pagamenti. Conservare l'analisi e i controlli compensativi come documento a sé stante e datato, collegandolo dalla Dichiarazione di Applicabilità.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.4 **Responsabilità della direzione: la direzione richiede a tutto il personale di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite.**

Come si dimostra: Un impegno nei contratti di lavoro e con i contrattisti, la presa visione delle politiche all'onboarding e promemoria periodici da parte della direzione. Evidenza: dichiarazioni di impegno firmate e verbali di riunione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.5 **Contatti con le autorità: sono mantenuti contatti appropriati con le autorità pertinenti e questi sono raggiungibili quando necessario.**

Come si dimostra: Un elenco di contatti con l'autorità di protezione dei dati competente, la polizia o l'unità cybercrime, il punto nazionale di segnalazione della sicurezza informatica e, ove pertinente, i canali di segnalazione NIS2. Annotare direttamente nell'elenco le scadenze (come le 72 ore del RGPD).

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.6 **Contatti con gruppi di interesse speciale: sono mantenuti contatti con gruppi di interesse speciale, forum sulla sicurezza e associazioni professionali.**

Come si dimostra: Iscrizioni, bollettini di allerta sottoscritti (CERT nazionale, avvisi dei fornitori), partecipazione a gruppi di interesse speciale. Un'evidenza semplice: un elenco di iscrizioni più un esempio di come un avviso abbia dato origine a un'azione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.7 **Intelligence sulle minacce: sono raccolte e analizzate informazioni sulle minacce alla sicurezza delle informazioni per derivarne azioni appropriate.**

Come si dimostra: Nuovo nell'edizione 2022. Praticabile per le organizzazioni piccole: iscriversi agli avvisi del CERT nazionale e dei fornitori, poi svolgere una breve rassegna mensile con una decisione di rilevanza e i ticket che ne derivano. L'evidenza è l'analisi, non l'iscrizione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.8 **Sicurezza delle informazioni nella gestione dei progetti: la sicurezza delle informazioni è integrata nella gestione dei progetti, indipendentemente dal tipo di progetto.**

Come si dimostra: Voci di sicurezza nella checklist di progetto: esigenze di protezione, riesame del rischio, verifica di protezione dei dati, avallo di sicurezza prima del go-live. Nei team agili ancorarle come voci fisse nella definizione di pronto e nella definizione di fatto.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.9 **Inventario delle informazioni e degli altri asset associati: è creato e mantenuto un inventario delle informazioni e degli altri asset associati con responsabili nominati.**

Come si dimostra: Un inventario degli asset che copra hardware, software, servizi cloud, archivi di dati, domini e account, ciascuno con un responsabile e le proprie esigenze di protezione. Nelle organizzazioni piccole può essere assemblato automaticamente a partire da un'esportazione MDM, un elenco licenze e la console cloud; una data aggiornata è obbligatoria.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.10 **Uso accettabile delle informazioni e degli altri asset associati: sono individuate, documentate e attuate regole per l'uso accettabile e la gestione delle informazioni e degli altri asset associati.** Documento

Come si dimostra: Una politica di uso accettabile per dispositivi, reti, account cloud e strumenti di IA, con presa visione. I dispositivi personali e i servizi di IA esterni vanno coperti esplicitamente, perché è lì che avviene la maggior parte delle fughe di dati.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.11 **Restituzione degli asset: quando un rapporto di lavoro termina o cambia, è disciplinato e confermato per iscritto che tutti i dispositivi, chiavi, account e documenti assegnati vengano restituiti.**

Come si dimostra: Una checklist di offboarding con ricevuta di restituzione per laptop, token, chiavi, certificati e supporti di memorizzazione, più la disattivazione degli account nello stesso giorno. Ciò vale allo stesso modo per liberi professionisti e stagisti.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.12 **Classificazione delle informazioni: le informazioni sono classificate in base alle proprie esigenze di protezione riguardo a riservatezza, integrità, disponibilità e requisiti di legge.**

Come si dimostra: Uno schema semplice con tre o quattro livelli (pubblico, interno, riservato, strettamente riservato) e regole di gestione concrete per livello. Registrare l'assegnazione nell'inventario degli asset o nel registro delle attività di trattamento.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.13 **Etichettatura delle informazioni: il livello di classificazione è riconoscibile sul documento, sul file o sul messaggio stesso, cosicché i destinatari sappiano come gestirlo senza dover chiedere.**

Come si dimostra: Etichettatura nell'intestazione del documento, nel nome del file, nell'oggetto dell'email o tramite etichette di sensibilità nella suite ufficio cloud. Evidenza tramite campioni di documenti effettivamente etichettati, non solo tramite la regola.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.14 **Trasferimento delle informazioni: sono in vigore regole, procedure e accordi per il trasferimento delle informazioni all'interno dell'organizzazione e con parti esterne.**

Come si dimostra: Una regola che indichi quale canale sia consentito per ciascun livello di classificazione: email cifrata o data room per i contenuti riservati, nessun invio tramite messaggistica privata. Sostenere i trasferimenti riservati con accordi di non divulgazione.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.15 **Controllo degli accessi: sono stabilite e attuate regole per controllare l'accesso fisico e logico alle informazioni e agli altri asset associati, basate sui requisiti di business e di sicurezza.**

Come si dimostra: Una politica di controllo degli accessi che segua il need to know e il minimo privilegio, con una corrispondenza ruolo-diritti. Evidenza tramite la configurazione effettiva dei diritti nel provider di identità, non solo tramite la politica.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.16 **Gestione delle identità: è gestito l'intero ciclo di vita delle identità.**

Come si dimostra: Un processo dalla creazione, passando per la modifica, fino alla disattivazione, idealmente centralizzato in un provider di identità con single sign-on. Nessun account di gruppo condiviso; dove tecnicamente inevitabile, nominare l'account, motivarlo e registrarne l'uso.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.17 **Informazioni di autenticazione: l'assegnazione e la gestione delle informazioni di autenticazione sono controllate da un processo di gestione che richiede alle persone di trattarle correttamente.**

Come si dimostra: Un gestore di password come strumento obbligatorio, una politica sulla qualità delle password e sulla MFA, un accesso iniziale sicuro e una procedura di reset con verifica dell'identità. Evidenza tramite schermate della configurazione e il rapporto del gestore di password.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.18 **Diritti di accesso: i diritti di accesso sono assegnati, riesaminati, modificati e rimossi in conformità con la politica di controllo degli accessi.**

Come si dimostra: Un riesame periodico degli accessi, almeno annuale, con un esito documentato per account e l'evidenza dei diritti rimossi. La rimozione il giorno stesso dell'uscita è un punto che agli auditor piace verificare con un caso concreto.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.19 **Sicurezza delle informazioni nei rapporti con i fornitori: sono definiti e attuati processi e procedure per gestire i rischi di sicurezza derivanti dall'uso di prodotti e servizi di terze parti.**

Come si dimostra: Un elenco fornitori con un livello di criticità e la profondità della valutazione. Per i fornitori critici ottenere evidenze (certificato ISO 27001, rapporto SOC 2) anziché condurre audit propri, che è l'unica via realistica per le organizzazioni piccole.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.20 **Gestione della sicurezza delle informazioni negli accordi con i fornitori: con ciascun fornitore sono concordati i requisiti di sicurezza rilevanti, riportati nei contratti.**

Come si dimostra: Un allegato contrattuale sulla sicurezza delle informazioni con obblighi di notifica degli incidenti, regole sui subresponsabili, obblighi di cancellazione e diritti di audit. Per i servizi standard sono sufficienti le condizioni del fornitore più un accordo sul trattamento dei dati, purché il loro contenuto sia stato riesaminato e documentato.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.21 **Gestione della sicurezza delle informazioni nella catena di fornitura ICT: sono definiti e attuati processi per gestire i rischi di sicurezza nella catena di fornitura delle tecnologie dell'informazione e della comunicazione.**

Come si dimostra: Questo copre le dipendenze software e i subfornitori dei fornitori stessi. In pratica: una distinta base del software (SBOM) o un elenco delle dipendenze, controlli automatizzati sui pacchetti vulnerabili nella CI, e approvvigionamento di software solo tramite canali firmati o ufficiali.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.22 **Monitoraggio, riesame e gestione dei cambiamenti dei servizi dei fornitori: i cambiamenti nei servizi dei fornitori sono regolarmente monitorati, riesaminati e gestiti.**

Come si dimostra: Un riesame annuale dei fornitori che consideri incidenti, rapporti sulla disponibilità e validità dei certificati, più un canale per gli annunci di cambiamento del fornitore. Registrare l'esito come breve nota per fornitore.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.23 **Sicurezza delle informazioni per l'uso di servizi cloud: sono stabiliti processi per acquisire, usare, gestire e uscire dai servizi cloud in linea con i requisiti di sicurezza.**

Come si dimostra: Nuovo nell'edizione 2022 e controllo centrale per le organizzazioni piccole basate sul cloud. Evidenza tramite una politica cloud con un processo di approvazione per i nuovi servizi, un modello di responsabilità condivisa documentato per servizio, impostazioni di hardening, e una strategia di uscita che includa la restituzione dei dati e la conferma della cancellazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.24 **Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni: sono pianificati e stabiliti processi, ruoli e responsabilità per la gestione degli incidenti.** Documento

Come si dimostra: Un piano di risposta agli incidenti con il percorso di notifica, i ruoli, i livelli di escalation, i contatti fuori orario e i modelli di comunicazione. Realistico per i team piccoli: una pagina, ma esercitata.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.25 **Valutazione e decisione sugli eventi di sicurezza delle informazioni: gli eventi di sicurezza sono valutati e viene decisa la loro classificazione come incidenti di sicurezza delle informazioni.**

Come si dimostra: Criteri di triage con una matrice di gravità e un registro degli eventi in cui compaiano con motivazione anche gli eventi scartati. La separazione tra evento e incidente deve essere visibile nel registro.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.26 **Risposta agli incidenti di sicurezza delle informazioni: gli incidenti sono gestiti in conformità con le procedure documentate.**

Come si dimostra: Fascicoli degli incidenti con una cronologia, le azioni intraprese, le persone coinvolte e la decisione di chiusura. Se non si è ancora verificato un incidente reale, un'esercitazione simulata documentata è la migliore evidenza disponibile.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.27 **Apprendimento dagli incidenti di sicurezza delle informazioni: la conoscenza acquisita dagli incidenti è utilizzata per rafforzare i controlli di sicurezza.**

Come si dimostra: Un riesame post-incidente senza ricerca di colpevoli, con analisi delle cause radice e azioni derivate, collegato al registro dei miglioramenti e, ove necessario, al registro dei rischi.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.28 **Raccolta delle evidenze: è disciplinato come le tracce relative a un evento di sicurezza siano identificate, messe in sicurezza e conservate, affinché rimangano utilizzabili in seguito.**

Come si dimostra: Una breve procedura di conservazione delle evidenze: non ricostruire prematuramente i sistemi, mettere in sicurezza immagini e log, documentare la catena di custodia. Per le organizzazioni piccole basta definire il livello di gravità a partire dal quale viene chiamato un fornitore forense esterno, insieme ai relativi contatti.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.29 **Sicurezza delle informazioni durante le interruzioni: l'organizzazione pianifica come mantenere la sicurezza delle informazioni a un livello appropriato durante un'interruzione.**

Come si dimostra: Le disposizioni di emergenza non devono disattivare la sicurezza. Documentare che MFA, registrazione delle attività e restrizioni di accesso si applicano anche nell'operatività di riserva, e che gli account di emergenza (account break-glass) sono sigillati, documentati e riesaminati in seguito.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.30 **Prontezza ICT per la continuità operativa: la prontezza ICT è pianificata, attuata, mantenuta e testata sulla base degli obiettivi di continuità operativa e dei requisiti di continuità ICT.**

Come si dimostra: Nuovo nell'edizione 2022. Evidenza tramite obiettivi di tempo di ripristino (RTO) e obiettivi di punto di ripristino (RPO) definiti per sistema critico, una procedura di ripristino e almeno un test documentato all'anno. Un test di ripristino riuscito con data e durata è la singola evidenza più solida.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.31 **Requisiti legali, statutari, regolamentari e contrattuali: sono individuati, documentati e mantenuti aggiornati i requisiti rilevanti e l'approccio per soddisfarli.** Documento

Come si dimostra: Un registro legale che copra RGPD, diritto delle telecomunicazioni, diritto commerciale e tributario e, ove applicabile, NIS2 o norme di settore specifiche, ciascuno con la regola che lo attua e la data di riesame. Un riesame annuale è sufficiente, ma deve essere datato.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.32 **Diritti di proprietà intellettuale: sono attuate procedure appropriate per proteggere i diritti di proprietà intellettuale.**

Come si dimostra: Un inventario delle licenze del software in uso, un controllo delle licenze open source nel prodotto (uno scanner di licenze nella CI) e una regola per la gestione del codice di terze parti e del codice generato. Evidenza: il rapporto sulle licenze proveniente dalla build.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.33 **Protezione delle registrazioni: le registrazioni aziendali e probatorie sono archiviate in modo da non poter andare perse, non poter essere alterate senza che ce ne si accorga e non poter finire in mani sbagliate, e ciò vale per l'intero periodo di conservazione.**

Come si dimostra: Un piano di conservazione con i termini di legge, archiviazione resistente a manomissioni, accesso ristretto e backup. Per le registrazioni rilevanti a fini fiscali indicare esplicitamente i termini di conservazione di legge, poiché agli auditor piace verificarlo in modo specifico.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.34 **Privacy e protezione dei dati personali (PII): sono individuati e soddisfatti, in conformità con la legge applicabile, i requisiti relativi alla privacy e alla protezione delle informazioni di identificazione personale (PII).**

Come si dimostra: Registro delle attività di trattamento, accordi sul trattamento dei dati, un concetto di cancellazione, un processo per i diritti degli interessati e, ove richiesto, una valutazione d'impatto sulla protezione dei dati. Collegare questo aspetto al SGSI tramite un elenco di asset condiviso evita di mantenere tutto in duplicato.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.5.35 **Riesame indipendente della sicurezza delle informazioni: l'approccio dell'organizzazione alla gestione della sicurezza delle informazioni è riesaminato in modo indipendente a intervalli pianificati e ogni volta che si verificano cambiamenti significativi.**

Come si dimostra: Si evidenzia tramite l'audit interno condotto da un auditor indipendente, tramite penetration test esterni o tramite lo stesso audit di certificazione. Indipendente significa non condotto dalla persona responsabile dell'area riesaminata.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.36 **Conformità alle politiche, alle regole e alle norme per la sicurezza delle informazioni: la conformità alle politiche di sicurezza proprie dell'organizzazione e alle norme applicabili è riesaminata regolarmente.**

Come si dimostra: Controlli di conformità con data ed esito, ad esempio un controllo di configurazione rispetto alla propria baseline di hardening, un campionamento dell'etichettatura dei documenti, controlli automatizzati delle politiche nel cloud. Le deviazioni alimentano il registro delle azioni correttive.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.5.37 **Procedure operative documentate: le procedure operative per le strutture di trattamento delle informazioni sono documentate e messe a disposizione delle persone che ne hanno bisogno.** Documento

Come si dimostra: Runbook per backup e ripristino, deployment, amministrazione utenti, applicazione delle patch e gestione degli incidenti. Breve e aggiornato supera esteso e obsoleto; una data di ultima modifica per runbook è obbligatoria.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.6 Allegato A: Controlli relativi alle persone 8

A.6.1 **Selezione: i candidati che devono lavorare per l'organizzazione sono sottoposti preventivamente a verifiche, entro i limiti di legge e in modo proporzionato alle esigenze di protezione; per i ruoli sensibili la verifica è ripetuta durante il rapporto di lavoro.**

Come si dimostra: In assenza di dipendenti questo controllo può essere motivato come attualmente non applicabile, ma la procedura per il caso di un'assunzione deve comunque essere definita e registrata nella Dichiarazione di Applicabilità come pianificata. Un campo di applicazione praticabile: verifica dell'identità, del curriculum e delle referenze, più certificati; un controllo del casellario giudiziale solo dove le esigenze di protezione lo giustifichino e la legge lo consenta. Richiedere lo stesso standard a liberi professionisti e contrattisti tramite i loro contratti, altrimenti la lacuna si apre esattamente lì.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.6.2 **Termini e condizioni di impiego: gli accordi contrattuali stabiliscono le responsabilità di sicurezza delle informazioni del personale e dell'organizzazione.**

Come si dimostra: Una clausola di sicurezza nel contratto di lavoro o di servizio che rimandi alle politiche applicabili. Per i liberi professionisti la stessa clausola nel contratto di servizio, più un accordo di riservatezza.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.6.3 **Consapevolezza, istruzione e formazione sulla sicurezza delle informazioni: il personale e le parti esterne pertinenti ricevono un'adeguata consapevolezza e formazione, nonché aggiornamenti regolari sulle politiche dell'organizzazione.**

Come si dimostra: Formazione annuale con evidenza di presenza e data, integrata da simulazioni di phishing con un tasso di clic valutato. Anche i liberi professionisti senza personale necessitano di evidenza della propria formazione continua, ad esempio conferme di corsi.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.6.4 **Processo disciplinare: esiste un processo formale e comunicato per intraprendere azioni nei confronti delle persone che hanno violato le politiche di sicurezza.**

Come si dimostra: In assenza di dipendenti questo può essere motivato come attualmente non applicabile, ma il processo deve comunque essere definito per il caso di un'assunzione; decade solo la sua applicazione, non la regola. È richiesta una scala di risposte graduata e comunicata (colloquio, richiamo, ammonimento formale, licenziamento) in conformità con il diritto del lavoro e le norme sulla rappresentanza del personale. Per i contrattisti, riflettere il livello sanzionatorio nel contratto, ad esempio una penale contrattuale o un diritto di recesso.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.6.5 **Responsabilità dopo la cessazione o il cambiamento del rapporto di lavoro: le responsabilità e gli obblighi di sicurezza che restano validi dopo la cessazione o un cambiamento di ruolo sono definiti, applicati e comunicati alle persone interessate.**

Come si dimostra: Una checklist di offboarding con revoca dei diritti, restituzione degli asset, passaggio di consegne e un promemoria esplicito degli obblighi di riservatezza che permangono. Un verbale firmato del colloquio di uscita è l'evidenza più semplice.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.6.6 **Accordi di riservatezza o di non divulgazione: è determinato chi deve firmare un accordo di riservatezza. Il contenuto corrisponde alle esigenze di protezione delle informazioni, gli accordi sono firmati, archiviati e riesaminati regolarmente per mantenerli aggiornati.**

Come si dimostra: Accordi di riservatezza firmati per dipendenti, liberi professionisti, fornitori di servizi e stagisti, con un periodo di ultrattività. Una tabella riepilogativa con controparte, data e validità rende il portafoglio verificabile in audit.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.6.7 **Lavoro da remoto: sono attuate misure di sicurezza laddove le persone lavorino al di fuori dei locali dell'organizzazione e accedano nel frattempo alle informazioni organizzative.**

Come si dimostra: Una politica per l'home office e il lavoro da remoto con requisiti su cifratura del disco, blocco schermo, Wi-Fi sicuro, uso di VPN o accesso a fiducia zero, filtri privacy e un divieto di usare dispositivi personali senza approvazione. Evidenza tramite il rapporto di conformità MDM per gli endpoint.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.6.8 **Segnalazione degli eventi di sicurezza delle informazioni: esiste un meccanismo tramite il quale le persone possono segnalare tempestivamente eventi di sicurezza osservati o sospetti.**

Come si dimostra: Un canale di segnalazione comunicato chiaramente (casella email, canale di chat, numero di telefono) con la garanzia di assenza di sanzioni per le segnalazioni in buona fede. Evidenza: il volume delle segnalazioni nel registro degli eventi; un registro permanentemente vuoto è un segnale d'allarme in audit.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7 Allegato A: Controlli fisici 14

A.7.1 **Perimetri di sicurezza fisica: sono definiti e utilizzati perimetri di sicurezza per proteggere le aree che contengono informazioni e strutture di trattamento delle informazioni.**

Come si dimostra: Una descrizione dei perimetri con uno schizzo o fotografie: edificio, ufficio, armadio server. In un home office il perimetro è la stanza di lavoro chiudibile a chiave o, in mancanza, un armadio chiudibile; descriverlo anziché ometterlo.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.2 **Ingresso fisico: le aree sicure sono protette da controlli d'ingresso e punti di accesso appropriati.**

Come si dimostra: Un registro chiavi o badge con consegna e restituzione, e una regola per i visitatori con accompagnamento e un log. Se si utilizza uno spazio di coworking o un data center, assumere come evidenza i controlli d'ingresso del gestore e assicurarli contrattualmente.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.3 **Messa in sicurezza di uffici, locali e strutture: la sicurezza fisica di uffici, locali e strutture è progettata e attuata.**

Come si dimostra: Porte chiudibili a chiave, protezione delle finestre al piano terra, nessuno schermo riservato visibile dall'esterno, nessuna insegna aziendale su aree sensibili. Una breve descrizione più una fotografia sono sufficienti come evidenza.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.4 **Monitoraggio della sicurezza fisica: i locali sono monitorati con continuità contro accessi fisici non autorizzati.**

Come si dimostra: Nuovo nell'edizione 2022. Le opzioni sono un sistema di allarme, rilevatori di movimento, videosorveglianza o registri d'ingresso. La videosorveglianza deve essere verificata quanto alla conformità con la protezione dei dati; in un home office l'alternativa motivata è una combinazione di sistema di allarme, stanza chiusa a chiave e la constatazione che lì non vengono conservati server sensibili.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.5 **Protezione contro minacce fisiche e ambientali: è predisposta una protezione contro minacce fisiche e ambientali, come disastri naturali e danni intenzionali o non intenzionali.**

Come si dimostra: Una rassegna di incendio, acqua, calore, interruzione di corrente e effrazione, insieme alle misure in atto (rilevatori di fumo, estintori, nessuna apparecchiatura sotto tubature d'acqua, backup conservato in un'ubicazione diversa). È qui che si collega la determinazione sul cambiamento climatico del punto 4.1.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.6 **Lavoro in aree sicure: sono progettate e attuate misure per il lavoro in aree sicure.**

Come si dimostra: Regole per la sala server o per aree ad alta riservatezza: nessun accesso di terzi non sorvegliato, nessuna registrazione con telecamere o dispositivi mobili, registrazione del lavoro svolto. Se non esistono aree sicure, ciò può essere motivato facendo riferimento a un'operatività esclusivamente cloud.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.7 **Scrivania pulita e schermo pulito: sono definite e seguite regole per una scrivania pulita riguardo a documenti cartacei e supporti rimovibili e per il blocco degli schermi.**

Come si dimostra: Questo si applica pienamente anche nell'home office e quindi non deve essere dichiarato non applicabile. Si evidenzia tramite una breve regola (documenti chiusi a chiave, blocco schermo dopo cinque minuti, nessun post-it con credenziali) più il blocco imposto tecnicamente tramite la politica dei dispositivi, la cui configurazione può essere esportata.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.8 **Posizionamento e protezione delle apparecchiature: le apparecchiature sono posizionate e protette in modo sicuro.**

Come si dimostra: Posizionamento lontano da zone di passaggio e aree pubbliche, nessuna visibilità dall'esterno, protezione da calore e umidità, cavi di sicurezza per i dispositivi mobili. Basta una breve descrizione all'interno della politica per l'home office o l'ufficio.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.9 **Sicurezza degli asset fuori sede: gli asset situati al di fuori dei locali sono protetti.**

Come si dimostra: Nelle organizzazioni piccole si tratta principalmente del laptop, dello smartphone e dei supporti esterni, e non può essere argomentato diversamente. Evidenza: cifratura del disco imposta, cancellazione da remoto abilitata tramite MDM, una regola contro il lasciare i dispositivi nei veicoli e contro l'uso di reti pubbliche senza VPN, più un percorso di segnalazione degli smarrimenti. Il rapporto di conformità MDM che mostra lo stato di cifratura per dispositivo è la singola evidenza più solida.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.10 **Supporti di memorizzazione: i supporti di memorizzazione sono gestiti lungo l'intero ciclo di vita in conformità con lo schema di classificazione e i requisiti di gestione, dall'acquisizione, passando per l'uso e il trasporto, fino allo smaltimento.**

Come si dimostra: Questo si applica anche al lavoro puramente mobile, perché esistono chiavette USB, dischi esterni e supporti di backup. Evidenza: un registro dei supporti, supporti cifrati, un divieto imposto tecnicamente di supporti rimovibili non approvati, conservazione sicura in un luogo chiudibile a chiave, e passaggio al punto A.7.14 a fine vita.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.11 **Servizi di supporto: le strutture di trattamento delle informazioni sono protette contro il guasto dei servizi di supporto, in particolare l'alimentazione elettrica.**

Come si dimostra: Dove i server sono gestiti in sede, un gruppo di continuità con un test documentato. In una configurazione esclusivamente cloud l'evidenza è il riferimento agli impegni del fornitore più una regola su come continuare a lavorare durante un'interruzione locale di corrente o internet (tethering mobile, sede alternativa).

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.12 **Sicurezza del cablaggio: il cablaggio di alimentazione, dati e comunicazioni è protetto contro intercettazione, interferenza e danneggiamento.**

Come si dimostra: Dove il cablaggio è di proprietà, protezione contro danni e contro l'accesso non autorizzato ai pannelli di permutazione. In piccoli uffici e home office la motivazione è essenziale, ma va comunque fornita: router e prese di rete non sono accessibili pubblicamente, le porte inutilizzate sono disabilitate.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.13 **Manutenzione delle apparecchiature: le apparecchiature sono mantenute correttamente per garantire la disponibilità, l'integrità e la riservatezza delle informazioni.**

Come si dimostra: Un piano di manutenzione o lo stato del supporto del fornitore per dispositivo, e una regola per le riparazioni effettuate da terzi (rimuovere prima il supporto di memorizzazione o cancellare i dati, e stipulare un accordo di riservatezza con il fornitore). Tracciare le date di fine supporto nell'inventario degli asset.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.7.14 **Smaltimento sicuro o riutilizzo delle apparecchiature: prima che un dispositivo contenente un supporto di memorizzazione sia ceduto, venduto o rottamato, è verificato e registrato che non possano più essere ricostruiti su di esso dati protetti né software con licenza.**

Come si dimostra: Questo si applica anche nell'home office e ai dispositivi personali dismessi che sono stati usati per il lavoro. Evidenza: un registro di cancellazione per dispositivo con numero di serie, data e metodo (crypto-erase su SSD cifrati, sovrascrittura, distruzione fisica), oppure un certificato di distruzione da un fornitore. Per i dispositivi cifrati basta la distruzione documentata della chiave, purché la procedura sia descritta.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8 Allegato A: Controlli tecnologici 34

A.8.1 Dispositivi endpoint utente: sono protette le informazioni memorizzate, trattate o accessibili tramite i dispositivi endpoint utente.

Come si dimostra: Una baseline di hardening per sistema operativo, gestione centralizzata tramite MDM, cifratura del disco, aggiornamenti automatici e blocco schermo. Il rapporto di conformità MDM con uno stato per dispositivo evidenzia tutto ciò in un'unica volta.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.2 Diritti di accesso privilegiato: l'assegnazione e l'uso dei diritti di accesso privilegiato sono limitati e gestiti.

Come si dimostra: Un elenco di tutti gli account amministratore con motivazione, account amministratore separati non usati per il lavoro quotidiano, MFA imposta, elevazione limitata nel tempo dove possibile, e riesame periodico. Nelle organizzazioni piccole è il controllo compensativo più importante per il punto A.5.3.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.3 Restrizione dell'accesso alle informazioni: l'accesso alle informazioni e agli altri asset associati è limitato in conformità con la politica di controllo degli accessi stabilita.

Come si dimostra: Un concetto di autorizzazione basato su ruoli e gruppi anziché concessioni individuali, evidenziato tramite un'esportazione delle appartenenze ai gruppi. Riesaminare regolarmente i link di condivisione pubblica nell'archiviazione cloud e lasciarli scadere.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.4 Accesso al codice sorgente: l'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software è gestito in modo appropriato.

Come si dimostra: Permessi del repository per ruolo, branch principali protetti, revisioni imposte o controlli di stato imposti, nessun push diretto sul branch principale. Evidenza tramite la configurazione di protezione dei branch e l'elenco dei membri dell'organizzazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.5 Autenticazione sicura: sono attuate tecnologie e procedure di autenticazione sicura sulla base delle restrizioni di accesso e della politica specifica per argomento.

Come si dimostra: MFA per tutti gli accessi esterni e tutti gli account amministratore, metodi resistenti al phishing (passkey, FIDO2) dove possibile, e blocco dopo tentativi falliti. Evidenza tramite il rapporto di copertura MFA del provider di identità.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.6 Gestione della capacità: sono monitorati archiviazione, capacità di calcolo, banda e licenze, e la domanda è adeguata con sufficiente anticipo affinché i colli di bottiglia non mettano mai a rischio la disponibilità.

Come si dimostra: Monitoraggio dell'archiviazione, del carico di calcolo, delle quote di licenza e dei budget cloud con avvisi di soglia. Nelle organizzazioni piccole bastano un avviso sull'uso del disco e sui limiti di costo, più una verifica annuale della capacità.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.7 Protezione contro il malware: le difese tecniche contro il malware sono attive e aggiornate, e le persone che usano i dispositivi sono formate a sufficienza da non indebolire tali difese.

Come si dimostra: Protezione attiva degli endpoint con una vista di stato centralizzata, un filtro email che ispeziona allegati e link, e una regola contro l'esecuzione di software non approvato. Il rapporto di stato datato della soluzione di protezione è l'evidenza diretta.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.8 **Gestione delle vulnerabilità tecniche: l'organizzazione si informa attivamente sulle vulnerabilità della tecnologia che utilizza, decide per ciascun rilievo quanto sia esposta e chiude la lacuna entro scadenze definite oppure motiva una risposta diversa.**

Come si dimostra: Gestione delle vulnerabilità con una fonte (scanner, controllo delle dipendenze in CI, avvisi dei fornitori), una valutazione di gravità e scadenze definite per livello, ad esempio critico entro 7 giorni. Evidenza: rapporti di scansione da più momenti nel tempo che mostrino la diminuzione dei rilievi aperti.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.9 **Gestione della configurazione: le configurazioni di hardware, software, servizi e reti, comprese le configurazioni di sicurezza, sono stabilite, documentate, attuate, monitorate e riesaminate.**

Come si dimostra: Nuovo nell'edizione 2022. Evidenza tramite configurazioni baseline documentate (baseline di hardening) e la loro applicazione forzata, idealmente come infrastructure as code nel controllo di versione o tramite profili MDM. Il rilevamento delle deviazioni e un confronto periodico delle configurazioni completano il quadro.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.10 **Cancellazione delle informazioni: le informazioni memorizzate nei sistemi informativi, sui dispositivi e sui supporti di memorizzazione sono cancellate non appena non sono più necessarie.**

Come si dimostra: Nuovo nell'edizione 2022 e strettamente legato al RGPD. Evidenza tramite un concetto di cancellazione con termini di conservazione per categoria di dati, politiche di conservazione attuate tecnicamente in servizi cloud e database, e log di cancellazione. Anche i backup e gli archivi di log necessitano di un termine di conservazione.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.11 **Mascheramento dei dati: il mascheramento dei dati è applicato in conformità con la politica specifica per argomento sul controllo degli accessi e con i requisiti di business e di legge.**

Come si dimostra: Nuovo nell'edizione 2022. In pratica: nessun dato di produzione negli ambienti di test e sviluppo, bensì dati anonimizzati o sintetici; pseudonimizzazione nell'analytics; mascheramento di numeri di conto e credenziali nei log e nelle interfacce di supporto. Evidenza tramite lo script o la procedura che genera i dati di test.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.12 **Prevenzione della fuga di dati: sono applicate misure di prevenzione della fuga di dati ai sistemi, alle reti e ai dispositivi che trattano, memorizzano o trasmettono informazioni sensibili.**

Come si dimostra: Nuovo nell'edizione 2022. Realistico nelle organizzazioni piccole: controllo dei link di condivisione nell'archiviazione cloud, blocco dei supporti rimovibili non approvati, regole contro l'inoltro a caselle personali, controlli sull'inserimento di dati riservati in servizi di IA esterni, e scansione dei segreti nel codice sorgente. Evidenza tramite la configurazione e tramite riesami dei riscontri.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.13 **Backup delle informazioni: esistono backup di dati, software e sistemi secondo una regola definita (ambito, frequenza, conservazione, ubicazione), e il ripristino da essi viene effettivamente testato a intervalli regolari.**

Come si dimostra: Una politica di backup con frequenza, conservazione e una copia offsite secondo il principio 3-2-1, cifratura dei backup, e protezione contro la sovrascrittura da ransomware (backup immutabili). Ciò che è decisivo è il test di ripristino documentato con data ed esito, perché un backup non testato viene considerato inesistente in audit.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.14 **Ridondanza delle strutture di trattamento delle informazioni: le strutture di trattamento delle informazioni sono attuate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità.**

Come si dimostra: La ridondanza deve corrispondere agli obiettivi di disponibilità, non al massimo possibile. Evidenza tramite una descrizione architetturale con istanze o zone ridondanti, dispositivi di scorta, e una decisione motivata su dove la ridondanza è deliberatamente assente.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.15 **Registrazione degli eventi: le attività rilevanti per la sicurezza lasciano una traccia. I log sono prodotti, conservati, protetti contro l'alterazione ed effettivamente analizzati, non solo raccolti.**

Come si dimostra: Registrare come minimo gli accessi e i tentativi falliti, le modifiche dei permessi, le azioni amministrative e l'accesso ai dati riservati. I log sono protetti contro l'alterazione e hanno un termine di conservazione definito; nelle organizzazioni piccole i log immutabili sono al tempo stesso la compensazione per la mancante separazione dei compiti di cui al punto A.5.3.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.16 **Attività di monitoraggio: reti, sistemi e applicazioni sono monitorati per rilevare comportamenti anomali e sono intraprese azioni appropriate per valutare potenziali incidenti di sicurezza.**

Come si dimostra: Nuovo nell'edizione 2022. Praticabile senza un team di sicurezza proprio: avvisi del provider di identità su spostamenti impossibili e su serie di tentativi falliti, avvisi della piattaforma cloud su spesa insolita o modifiche dei permessi, inoltrati a una casella supervisionata con un tempo di risposta definito. Evidenza tramite le regole di allerta più esempi di allerte gestite.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.17 **Sincronizzazione degli orologi: tutti i sistemi che scrivono log traggono il proprio orario da una fonte definita e affidabile, cosicché gli eventi possano essere ordinati correttamente tra sistemi diversi.**

Come si dimostra: Configurazione NTP su server ed endpoint, e un fuso orario uniforme nei log (idealmente UTC). Senza sincronizzazione dell'orario, la ricostruzione di un incidente ai sensi del punto A.5.28 non regge; un estratto di configurazione è sufficiente come evidenza.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.18 **Uso di programmi di utilità privilegiati: l'uso di programmi di utilità in grado di annullare le protezioni di sistema è limitato e strettamente controllato.**

Come si dimostra: Un elenco degli strumenti di amministrazione approvati, restrizione dei diritti di amministratore locale, controllo delle applicazioni (allowlisting) dove possibile, e registrazione dell'uso. Evidenza: la politica più la configurazione della gestione dei diritti.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.19 **Installazione del software sui sistemi operativi: sono attuate procedure e misure per gestire in modo sicuro l'installazione del software sui sistemi operativi.**

Come si dimostra: Solo software approvato proveniente da fonti attendibili, installazione tramite distribuzione centralizzata o un gestore di pacchetti, un percorso di rollback e conservazione della versione precedente. Evidenza tramite l'elenco di approvazione e i log di deployment.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.20 **Sicurezza delle reti: le reti e i dispositivi di rete attivi hanno un responsabile nominato, una configurazione irrobustita e un insieme di regole tracciabile che definisce quale traffico sia consentito in assoluto.**

Come si dimostra: Un insieme di regole del firewall che segue il principio del deny by default, porte aperte documentate con motivazione, una configurazione Wi-Fi sicura, e credenziali predefinite modificate sui dispositivi di rete. Evidenza tramite un'esportazione dell'insieme di regole e una scansione delle porte esterna.

◯ Aperto ◯ In corso ◯ Soddisfatto ◯ Non applicabile

Evidenza / motivazione

A.8.21 **Sicurezza dei servizi di rete: sono individuati, attuati e monitorati i meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione dei servizi di rete.**

Come si dimostra: Per ciascun servizio di rete in uso (VPN, DNS, posta, CDN) documentare gli impegni di sicurezza e la propria configurazione, compresa la cifratura in transito e gli impegni di livello di servizio del fornitore. Evidenza: una panoramica della configurazione più il contratto o la descrizione del servizio.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.22 **Segregazione delle reti: la rete è suddivisa in zone in modo che servizi, gruppi di utenti e sistemi con diverse esigenze di protezione non possano raggiungersi reciprocamente senza filtro.**

Come si dimostra: Segmenti di rete o VLAN separati per ospiti, amministrazione e produzione; nel cloud, account o reti virtuali separati con gruppi di sicurezza. In un home office l'attuazione praticabile è una rete o VLAN separata per i dispositivi di lavoro, tenuta distinta dai dispositivi personali e dalla domotica.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.23 **Filtraggio web: l'accesso a siti web esterni è gestito per ridurre l'esposizione a contenuti dannosi.**

Come si dimostra: Nuovo nell'edizione 2022. Raggiungibile con poco sforzo tramite un servizio DNS con filtraggio o il filtraggio web incluso nella protezione endpoint, con categorie bloccate e registrazione delle richieste bloccate. Evidenza tramite la configurazione del filtro e un estratto di reportistica.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.24 **Uso della crittografia: è definito in modo vincolante dove si applica la cifratura, con quali algoritmi, e come le chiavi sono generate, memorizzate, ruotate e distrutte lungo l'intero ciclo di vita.** Documento

Come si dimostra: Una politica di crittografia con algoritmi approvati e lunghezze minime delle chiavi, cifratura in transito (TLS) e a riposo, più una procedura di gestione delle chiavi che copra generazione, memorizzazione, rotazione e distruzione. Evidenza tramite la politica più la configurazione del servizio di chiavi o del vault.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.25 **Ciclo di vita di sviluppo sicuro: sono stabilite e applicate regole per lo sviluppo sicuro di software e sistemi.**

Come si dimostra: Una descrizione del processo di sviluppo con punti di controllo di sicurezza per fase: requisiti, progettazione, implementazione, test, rilascio, esercizio. Per i team piccoli basta una singola pagina che rimandi ai gate concreti della CI e all'obbligo di revisione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.26 **Requisiti di sicurezza delle applicazioni: i requisiti di sicurezza per le applicazioni sono individuati, specificati e approvati durante lo sviluppo e l'acquisizione.**

Come si dimostra: Requisiti di sicurezza come voci esplicite nell'elenco dei requisiti o come checklist riutilizzabile, orientata ad esempio a standard comuni di verifica della sicurezza applicativa. Evidenza tramite ticket o documenti di requisiti con un risvolto di sicurezza.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.27 **Architettura di sistema sicura e principi di ingegneria: sono stabiliti, documentati e applicati alle attività di sviluppo principi di ingegneria dei sistemi sicuri.**

Come si dimostra: Principi documentati come minimo privilegio, difesa in profondità, impostazioni predefinite sicure, minimizzazione dei dati e un approccio a fiducia zero, insieme alla loro applicazione visibile in schizzi architetturali o registri delle decisioni.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.28 **Codifica sicura: nello sviluppo software sono applicati principi di codifica sicura.**

Come si dimostra: Nuovo nell'edizione 2022. Evidenza tramite regole di codifica vincolanti, analisi statica del codice e scansione dei segreti come gate obbligatori nella CI, uso di librerie verificate, e revisioni del codice documentate. Dove la separazione dei compiti è impossibile, gate automatizzati imposti prendono il posto della revisione a quattro occhi; motivare ed evidenziare questo aspetto con la configurazione della pipeline.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.29 **Test di sicurezza in sviluppo e accettazione: sono definiti e attuati processi di test di sicurezza nell'ambito del ciclo di vita di sviluppo.**

Come si dimostra: Test di sicurezza automatizzati nella pipeline (controlli delle dipendenze, analisi statica e dinamica) più un penetration test periodico dove le esigenze di protezione sono elevate. Evidenza tramite rapporti di test datati e il tracciamento dei rilievi.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.30 **Sviluppo esternalizzato: le attività di sviluppo esternalizzate sono dirette, supervisionate e riesaminate.**

Come si dimostra: Dove lo sviluppo è esternalizzato, stabilire nel contratto i requisiti di sicurezza, assicurare la titolarità del codice e il diritto di revisione, ed effettuare revisioni del codice e test di sicurezza prima dell'accettazione. In assenza di sviluppo esternalizzato, la non applicabilità deve essere motivata in modo coerente nella SoA.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.31 **Separazione degli ambienti di sviluppo, test e produzione: gli ambienti di sviluppo, test e produzione sono separati e protetti.**

Come si dimostra: Account, progetti o namespace separati, credenziali separate e set di dati separati. In combinazione con il punto A.8.11, assicurarsi che nessun dato di produzione finisca in ambienti non di produzione. Evidenza tramite la panoramica degli ambienti e l'assegnazione dei diritti.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.32 **Gestione dei cambiamenti: i cambiamenti alle strutture di trattamento delle informazioni e ai sistemi informativi sono soggetti a procedure di gestione dei cambiamenti.**

Come si dimostra: Un processo di gestione dei cambiamenti con richiesta, valutazione d'impatto, test, approvazione, attuazione e un percorso di rollback. Nei team di sviluppo, una pipeline di pull request con controlli imposti e deployment registrati soddisfa questo punto, purché la cronologia sia immutabile.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.33 **Informazioni di test: le informazioni di test sono selezionate, protette e gestite in modo appropriato.**

Come si dimostra: Il principio: nessun dato personale reale nei sistemi di test. Dove ciò è inevitabile, documentare l'approvazione, il mascheramento, la restrizione dell'accesso e la cancellazione dopo il test. Evidenza tramite il concetto di dati di test e i log di cancellazione.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione

A.8.34 **Protezione dei sistemi informativi durante i test di audit: i test di audit che comportano l'accesso ai sistemi operativi sono pianificati e concordati con la direzione per evitare interruzioni dell'operatività.**

Come si dimostra: Un accordo di audit con una finestra temporale, un ambito, accesso in sola lettura dove possibile, registrazione dell'accesso di audit e approvazione della direzione. Ciò vale anche per i penetration test: un'autorizzazione di test scritta con una finestra temporale e un contatto di emergenza è l'evidenza.

○ Aperto ○ In corso ○ Soddisfatto ○ Non applicabile

Evidenza / motivazione