Requisiti di sicurezza per i fornitori di Alludo

Contenuti

Introduzione

Il presente documento definisce le pratiche delle aziende del Gruppo Alludo (collettivamente "Alludo") in materia di sicurezza delle informazioni, continuità operativa e privacy, nonché il programma di valutazione delle misure di sicurezza e continuità dei fornitori di Alludo. I processi, le procedure, i requisiti e gli obblighi menzionati nel presente documento sono collettivamente definiti "Standard di Alludo".

Il presente **Documento con i requisiti di sicurezza per i fornitori** informa i fornitori di beni e servizi (i "Fornitori") sulle esigenze in termini di sicurezza, continuità operativa e privacy delle quali Alludo li ritiene responsabili nell'ambito della fornitura dei servizi. I fornitori devono rispettare tali requisiti seguendo le best practice di settore e le proprie politiche di sicurezza aziendale. Alludo non sarà responsabile dei problemi riscontrati dai fornitori, inclusi la perdita di dati o i danni materiali, indipendentemente dalla causa.

In caso di discordanze fra il presente documento e un contratto scritto, i termini del contratto scritto prevarranno. I fornitori devono inoltre conformarsi con tutti i requisiti normativi locali, nazionali o regionali. In caso di conflitto fra il presente documento e le normative applicabili, i fornitori devono informare Alludo e proporre controlli alternativi per garantire norme equivalenti in materia di sicurezza, continuità o privacy.

Panoramica dei requisiti di sicurezza per i fornitori

Alludo è responsabile della protezione delle proprie informazioni riservate e a diffusione limitata dall'accesso o la divulgazione non autorizzati. A tale scopo, Alludo adotta gli Standard di Alludo, norme interne per la sicurezza delle informazioni, la continuità operativa e la privacy, per garantire che tali informazioni riservate e a diffusione limitata siano protette e che i servizi forniti da Alludo siano costantemente disponibili. Per garantire la conformità di Alludo alle norme interne e ai requisiti normativi in materia di sicurezza delle informazioni e continuità operativa, Alludo richiede ai propri fornitori di aderire agli Standard di Alludo descritti nel presente documento.

Di conseguenza, nella misura in cui un fornitore deleghi o subappalti in parte i propri obblighi ai sensi del proprio accordo con Alludo o ingaggi un altro fornitore per fornire i servizi direttamente o indirettamente ad Alludo, il fornitore dovrà richiedere a tale fornitore di implementare e gestire un piano e un programma di protezione delle informazioni conforme agli Standard di Alludo. Alludo si impegna a lavorare ragionevolmente con i propri fornitori per aiutarli a soddisfare i requisiti di conformità relativi agli Standard di Alludo. L'applicabilità degli Standard di Alludo a uno specifico fornitore dipenderà dai tipo di servizio e prodotto fornito da tale fornitore ad Alludo.

Controllo delle identità e degli accessi

Il fornitore deve garantire quanto segue:

1. **Controllo degli accessi e gestione degli utenti**:
   - 1.1. È predisposta una politica documentata di controllo degli accessi, aggiornata almeno una volta all'anno.
   - 1.2. I ruoli, le autorizzazioni e i diritti di accesso degli utenti sono definiti e documentati.
   - 1.3. Sono predisposti processi standard di onboarding e offboarding degli utenti, fra cui la tenuta dei registri delle approvazioni rilevanti.
   - 1.4. L'accesso ai componenti dell'infrastruttura IT è garantito in base al principio del privilegio minimo e gestito attraverso strumenti di gestione delle identità (Active Directory, OKTA o simili).
   - 1.5. L'accesso individuale ai sistemi, alle risorse di rete e ad altre risorse IT viene formalmente approvato e controllato attraverso ID utente univoci e password personali.
   - 1.6. La separazione delle funzioni viene mantenuta durante la creazione/la modifica degli ID utente e l'assegnazione dei privilegi.

2. **Politiche relative alla password e all'autenticazione**:
   - 2.1. Gli utenti sono tenuti a modificare la propria password al momento dell'accesso iniziale.

2.2. Le password devono rispettare i requisiti standard di settore per quanto riguarda la lunghezza, la scadenza, la complessità, la cronologia delle password, i tentativi non riusciti, la durata del blocco dell'account, la vita della password e la modifica al primo accesso.
2.3. Per fornire le password degli utenti e convalidare la loro identità prima della reimpostazione della password vengono usati meccanismi sicuri.
2.4. I sistemi che non supportano l'autenticazione IdP o che devono essere sviluppati in autonomia sono configurati in modo da applicare un'autenticazione forte, non inferiore alla configurazione definita nelle politiche centrali di controllo degli accessi e delle password.
2.5. Tutti i sistemi e le applicazioni sono configurati in modo da usare procedure di accesso sicure tramite meccanismi approvati di gestione degli accessi e delle identità.
2.6. I sistemi e le applicazioni sono configurati in modo tale che le sessioni inattive scadano, per evitare accessi non autorizzati.

3. **Gestione degli accessi privilegiati**:
   3.1. L'accesso privilegiato alla risorse è limitato a ruoli utente specifici e approvati dal personale autorizzato.
   3.2. Gli account utente privilegiati sono configurati per l'uso dell'autenticazione a più fattori.
   3.3. I privilegi non più necessari vengono revocati immediatamente.
   3.4. L'uso di credenziali amministrative è limitato a particolari circostanze, come la risoluzione dei problemi, e gli utenti eseguono le operazioni quotidiane con credenziali con meno privilegi.
   3.5. L'accesso a infrastrutture IT, sistemi, dispositivi di rete e applicazioni critiche (accesso remoto, server critici, dispositivi di rete) è protetto usando l'autenticazione a più fattori.

4. **Revisione e monitoraggio degli accessi**:
   4.1. Vengono svolte periodicamente revisioni dei diritti di accesso e le eccezioni identificate vengono gestite tempestivamente.
   4.2. Al massimo una volta all'anno, viene condotta una riconciliazione degli ID utente (inclusi domini, applicazioni, dispositivi di rete, sistemi IT, middleware, database, ecc.) e vengono intraprese immediatamente azioni correttive per tutte le anomalie identificate.
5. **Gestione di terzi e dei fornitori**:
   5.1. L'accesso dei fornitori terzi alle reti e ai sistemi è rigidamente controllato, in base al principio del "need to know" e dell'approvazione formale.
   5.2. Le credenziali predefinite date dai fornitori vengono modificate prima che i sistemi, le applicazioni, i dispositivi di rete o altri dispositivi dell'infrastruttura IT vengano messi in produzione.

6. **Considerazioni speciali in materia di accesso**:
   6.1. Non vengono usati ID generici e condivisi a meno che non siano formalmente giustificati e approvati dall'alta dirigenza con meccanismi che permettono di tracciarne l'uso e di risalire agli individui.
   6.2. Qualsiasi accesso in modalità amministratore senza console viene crittografato usando algoritmi di crittografia approvati dal settore, mentre i protocolli non sicuri (telnet/ftp) sono vietati per l'accesso in modalità amministratore senza console.

Gestione delle risorse

Il fornitore deve garantire quanto segue:

7. **Gestione e inventario delle risorse**:
   - 7.1. Vengono aggiornati inventari delle risorse completi che contengono dettagli essenziali quali il nome del proprietario, i dati di contatto e il luogo.
   - 7.2. I registri delle risorse informatiche, che includono hardware, sistemi operativi, applicazioni e database, vengono regolarmente aggiornati e verificati per garantirne l'accuratezza.
   - 7.3. Sono stati istituiti procedure di gestione delle risorse e controlli della configurazione per gestire la disponibilità delle risorse critiche e le configurazioni di reti e sistemi informativi determinanti.

8. **Classificazione e identificazione delle informazioni**:
   - 8.1. È in atto una politica di classificazione delle informazioni con procedure e linee guida di supporto. Tutte le risorse sono identificate sulla base di istruzioni definite e le informazioni vengono classificate e protette in base a livelli di classificazione definiti.

9. **Manipolazione delle risorse**:
   - 9.1. Sono in uso linee guida di gestione delle risorse per una manipolazione corretta e vengono comunicate a tutti i dipendenti e gli appaltatori interessati.
   - 9.2. Sono in atto procedure documentate per proteggere le risorse informative, identificare le risorse da eliminare e garantirne un'eliminazione sicura.
   - 9.3. Sono stati definiti processi per garantire che le risorse assegnate siano tempestivamente rese al team di gestione delle risorse corrispondente prima della chiusura del rapporto di lavoro, del contratto o dell'accordo.

10. **Gestione dei dispositivi mobili e dei supporti removibili**:
    - 10.1. Sono state implementate politiche e procedure per controllare i dispositivi mobili (inclusi BYOD) usati per archiviare, trasmettere o trattare informazioni aziendali. Prima di consentire l'accesso dei dispositivi mobili alle informazioni e risorse aziendali è necessaria l'adozione di misure di protezione adeguate.
    - 10.2. L'uso di dispositivi di archiviazione di massa removibili deve essere crittografato per garantire la sicurezza dei dati.

11. **Conformità del software**:
    - 11.1. È vietato l'uso di software senza licenza o non approvato. Sono in uso processi per identificare qualsiasi violazione e assumere le azioni necessarie per farvi fronte.

Operazioni IT

Il fornitore deve garantire quanto segue:

12. **Operazioni di sistema critiche**:

12.1. Sono state definite e vengono impiegate procedure per l'uso di sistemi informativi e reti critici che comprendono:

12.1.1. Processi di approvazione formale per l'accesso alle risorse IT.

12.1.2. Solidi meccanismi di autenticazione per tutte le tecnologie (VPN, accesso a Windows).

12.1.3. Revisione regolare dei diritti di privilegio.

12.1.4. Identificazione dei percorsi di rete per le tecnologie critiche sulla base dei requisiti di continuità aziendale.

13. **Gestione delle modifiche**:

13.1. È stato implementato un processo di gestione delle modifiche completo per i sistemi IT, le applicazioni, i database e i componenti di rete che permette:

13.1.1. L'accesso, la revisione, il test e l'approvazione formale di tutte le modifiche.

13.1.2. Piani di ripristino in caso di modifiche potenzialmente distruttive.

14. **Altro**:

14.1. I sistemi e i componenti di rete che gestiscono informazioni sensibili e riservate sono soggetti a verifiche di monitoraggio dell'integrità dei file.

14.2. Tutti i sistemi e i componenti di rete sono configurati per usare fonti NTP (Network Time Protocol) per una precisa sincronizzazione dell'ora.

14.3. Sono stati definiti regolari processi di manutenzione attivi e preventivi per tutti i sistemi critici, le applicazioni, i dispositivi di rete e le macchine degli utenti finali.

14.4. I set di regole per il firewall e il router vengono rivisti periodicamente o secondo quanto previsto dagli standard di settore, e le regole non necessarie o non autorizzate vengono tempestivamente rimosse.

14.5. Sono stati implementati controlli per mantenere l'integrità delle informazioni e del software in tutto l'ambiente IT.

Sicurezza delle risorse umane

Il fornitore deve garantire quanto segue:

15. **Controllo dei precedenti**:

15.1. Definire e garantire politiche e procedure per condurre il controllo dei precedenti.

15.2. Effettuare controlli dei precedenti appropriati sui dipendenti e gli appaltatori prima dell'onboarding, nella misura consentita dalla legge, in base alle loro funzioni e responsabilità.

16. **Gestione del cambio del personale**:

16.1. Implementare un processo per gestire i cambi del personale o dei loro ruoli e delle loro responsabilità, compresa la formazione del nuovo personale sulle politiche e le procedure rilevanti.

16.2. Revocare i diritti di accesso, i badge, le dotazioni e altre risorse subito dopo i cambi del personale quando non sono più necessari o permessi.

17. **Applicazione delle politiche**:

17.1. Implementare e garantire un processo disciplinare chiaro per i dipendenti che violano le politiche di sicurezza.
17.2. Garantire l'assunzione di responsabilità per le violazioni delle politiche di sicurezza attraverso misure contrattuali appropriate. A tale fine è compresa l'aggiunta di clausole rilevanti nei contratti di lavoro per il personale e negli accordi di servizio per gli appaltatori terzi.

Formazione sulla sicurezza e la privacy

Il fornitore deve garantire quanto segue:

18. La formazione sulla sicurezza e la privacy è obbligatoria per tutti i dipendenti e gli appaltatori. La formazione deve essere completata al momento dell'assunzione e, successivamente, rinnovata annualmente o con frequenza minore.
19. I dipendenti e gli appaltatori che assumono rilevanti responsabilità per la sicurezza IT devono completare una formazione annuale specializzata su misura in base ai loro specifici ruoli e compiti.
20. Il management ha accesso a strumenti e sistemi che gli consentono di monitorare i progressi formativi dei loro dipendenti e appaltatori.
21. Il programma di formazione e sensibilizzazione è sottoposto a revisioni e aggiornamenti periodici. Questo processo tiene conto dell'evoluzione dei requisiti aziendali, delle modifiche legislative e delle lezioni apprese dai passati incidenti a livello di sicurezza.

Sicurezza delle informazioni e governance

Il fornitore deve garantire quanto segue:

22. Framework di sicurezza e governance:
22.1. Il fornitore deve implementare un framework normativo sulla sicurezza riconosciuto (NIST CSF, RMF, 800-53, ISO 27001, CIS) per la governance delle informazioni e della sicurezza informatica. Il framework deve includere:
22.1.1. Politiche e procedure complete sulle informazioni e la sicurezza informatica soggette a revisione annuale, approvazione formale e comunicazione all'interno dell'intera azienda.
22.1.2. Una strategia di sicurezza delle informazioni ben definita allineata con gli obiettivi aziendali.
22.1.3. Solidi processi di governance e gestione dei rischi specificamente incentrati sulle informazioni e la sicurezza informatica.
22.1.4. Meccanismi di conformità per rispondere ai requisiti legali e normativi riguardanti le informazioni e la sicurezza informatica.
22.2. Se non aderisce a un framework di sicurezza riconosciuto, il fornitore deve inviare un report nel quale dimostra che il proprio ambiente è stato sottosposto ad audit.
22.2.1. Fra il fornitore e Alludo deve essere concordato un piano di correzione per i problemi identificati, incluse le tempistiche previste.

23. Leadership e struttura organizzativa:

23.1. I ruoli e le responsabilità appropriati per la sicurezza delle informazioni e informatica sono definiti e implementati all'interno dell'organizzazione.

24. Gestione e valutazione dei rischi:

24.1. È stato predisposto un framework di gestione dei rischi formale approvato dall'alta dirigenza per:

24.1.1. Identificare le minacce interne ed esterne.

24.1.2. Valutare la riservatezza delle informazioni/dei dati considerati.

24.1.3. Valutare potenziali impatti commerciali.

24.1.4. Valutare minacce, vulnerabilità e rischi corrispondenti.

24.1.4.1. Tutti i rischi e le minacce identificati vengono organizzati secondo priorità per prendere provvedimenti tempestivi al fine di mitigare i rischi.

24.1.4.2. Sono stati implementati processi e/o strumenti per identificare gli eventi che causano interruzioni nelle attività principali dell'azienda.

24.1.4.3. Il fornitore deve informare immediatamente Alludo qualora non sia in grado di rimediare o ridurre qualsiasi rischio materiale che potrebbe avere un impatto sul servizio fornito.

25. Compliance e monitoraggio delle prestazioni:

25.1. Sono in atto processi per identificare, registrare e tracciare tutti i requisiti legali, normativi e contrattuali applicabili all'azienda.

25.2. Vengono effettuate valutazioni periodiche per confermare la conformità agli obblighi legali, normativi e contrattuali. Vengono tenuti registri di tali valutazioni e identificate e attenuate tempestivamente eventuali lacune.

25.3. Le politiche, le procedure e le linee guida vengono riviste almeno una volta l'anno e aggiornate come da requisiti legali, normativi e contrattuali.

25.4. I KPI delle funzioni chiave, quali l'IT, la sicurezza delle informazioni e la privacy dei dati, sono definiti, formalmente documentati, periodicamente valutati e riportati all'alta dirigenza.

Sicurezza di rete

Il fornitore deve garantire quanto segue:

26. Progettazione della rete e architettura di sicurezza:

26.1. La rete del fornitore utilizza principi di "difesa in profondità", includendo controlli appropriati come la segmentazione della rete per ridurre le violazioni delle informazioni e della sicurezza informatica.

26.2. È implementata una forte progettazione dell'architettura con una gestione efficace delle identità e solide configurazioni del sistema operativo.

26.3. La progettazione e l'implementazione di rete sono sottoposte a revisioni annuali per garantire costante efficacia e sicurezza.

26.4. La configurazione di rete è conforme ai requisiti legali e normativi applicabili.

27. Controllo degli accessi e autenticazione:

27.1. Le connessioni di rete esterne devono essere documentate, instradate tramite firewall, verificate e approvate prima di poter essere stabilite.
27.2. L'accesso alla rete wireless richiede l'autenticazione, l'autorizzazione, la segmentazione e la crittografia. Sono presenti sistemi per rilevare i punti di accesso wireless non autorizzati o le connessioni non autorizzate e rispondervi.
27.3. L'accesso da remoto alla rete del fornitore deve essere approvato e condotto tramite mezzi sicuri, con l'autenticazione a più fattori.
27.4. Sono in uso controlli per prevenire o ridurre l'accesso non autorizzato alla rete del fornitore.

28. Amministrazione e gestione sicure:
28.1. Tutto il traffico di rete relativo alla gestione fra le workstation di amministrazione e i dispositivi di rete usano la crittografia standard di settore e i protocolli di autenticazione.
28.2. L'accesso dell'amministratore senza console avviene esclusivamente tramite canali crittografati approvati nel settore.
28.3. Gli account guest sono disattivati o rimossi e tutte le password predefinite e definite dal fornitore vengono modificate prima che i dispositivi di rete vengano distribuiti nell'ambiente di produzione.

29. Rafforzamento della rete e protezione dalle minacce:
29.1. I servizi, le applicazioni e le porte non utilizzati vengono disattivati per ridurre la superficie di attacco.
29.2. Per i segmenti di rete critici, vengono adottate misure di rilevamento e/o prevenzione delle intrusioni.
29.3. I sistemi critici vengono protetti da attacchi Denial of Service (DoS) e Distributed Denial of Service (DDoS).

Crittografia

Il fornitore deve garantire quanto segue:

30. È stata implementata una politica di crittografia completa, oltre a procedure di supporto, per garantire la conformità con tutti i requisiti legali, normativi e aziendali. Tale politica segue le best practice di settore per garantire la crittografia sicura in accordo con le leggi e gli standard applicabili.

31. Standard di crittografia e implementazione:
31.1. Sono autorizzati solo algoritmi di crittografia e livelli di sicurezza approvati dal settore a garanzia di una protezione dei dati adeguata per tutti i sistemi e processi.
31.2. Sono state implementate soluzioni di crittografia per proteggere le informazioni confidenziali e limitare l'accesso ai dati riservati, fra cui la crittografia per i dati sia in transito che a riposo.
31.3. Tutte le operazioni di archiviazione e trasmissione delle password sono crittografate al fine di assicurare sempre la riservatezza delle credenziali utente.
31.4. I dati di Alludo in transito devono essere crittografati (almeno (TLS 1.2 o standard più recente).

31.5. I dati di Alludo a riposo devono essere crittografati (almeno (AES 256 o standard più recente).

Protezione dei dati

Il fornitore deve garantire quanto segue:

32. Ripristino:

32.1. **Backup e ripristino dei dati**:

32.1.1. I backup dei dati di Alludo devono essere effettuati periodicamente.

32.1.2. I backup dei dati di Alludo devono essere conservati per 1 anno.

32.1.3. I backup dei dati di Alludo devono essere effettuati periodicamente.

32.2. **Disaster recovery**:

32.2.1. Il piano di disaster recovery deve essere testato ogni anno.

33. Politiche e procedure di backup:

33.1. La politica di backup e le procedure di supporto devono essere documentate chiaramente.

33.2. I processi di recupero dei backup devono essere documentati e testati secondo una frequenza definita.

33.3. Le prove dei test di recupero dei backup devono essere conservate.

33.4. Occorre conservare in sicurezza una copia dei file di backup di dati critici.

34. Monitoraggio del backup:

34.1. I registri dei backup non riusciti (se presenti) devono essere monitorati dall'amministratore del backup.

34.2. Per i backup non riusciti occorre eseguire e documentare azioni correttive.

35. Collocazione dei dati:

35.1. Il fornitore è responsabile di garantire la conformità con tutte le leggi sulla privacy e la protezione dei dati vigenti nei Paesi in cui i dati saranno archiviati.

35.2. Deve aderire alle restrizioni sul trasferimento dei dati oltre i confini (GDPR, ecc.).

35.3. Il fornitore deve implementare misure di sicurezza tecniche e organizzative appropriate per proteggere i dati in accordo con le leggi e gli standard dei Paesi in cui i dati vengono archiviati.

35.4. Alludo si riserva il diritto di controllare le pratiche di trattamento dei dati del fornitore per garantire la conformità con le misure di sicurezza e le normative locali concordate.

36. Cancellazione dei dati:

36.1. È necessario che siano in atto procedure per la cancellazione sicura dei dati alla conclusione del contratto, garantendo la conformità con le leggi sulla conservazione dei dati locali.

37. Crittografia completa del disco:

37.1. Per le workstation e i server deve essere configurata la crittografia completa del disco.

38. **Classificazione dei dati**:
    38.1. È necessario che sia in atto una politica di classificazione dei dati documentata.
    38.2. I dati devono essere classificati in base alla loro criticità e sensibilità.
    38.3. È necessario identificare e implementare controlli di sicurezza corrispondenti alla sensibilità dei dati.

Comunicazione delle informazioni

Il fornitore deve garantire quanto segue:

39. **Sicurezza web**:
    39.1. Un software di filtraggio dei contenuti è predisposto per bloccare l'accesso ai siti web che ospitano contenuti malevoli.
    39.2. L'accesso a tutti i sistemi e le applicazioni basati su web deve avvenire tramite meccanismi sicuri e autenticati.
    39.3. La comunicazione client-server per le applicazioni e i portali web deve avvenire su canali crittografati.

40. **Sicurezza delle e-mail**:
    40.1. Sono in atto controlli di sicurezza per prevenire l'uso improprio del sistema di posta elettronica.
    40.2. Tutte le comunicazione via e-mail devono essere trasmesse su canali crittografati.
    40.3. Il gateway di posta è dotato di:
        40.3.1. Filtri anti-phishing.
        40.3.2. Protocolli di sicurezza attivati per le e-mail (ad es. DMARC, DKIM e SPF).
        40.3.3. Altre configurazioni necessarie per prevenire minacce trasmesse via e-mail.

Sviluppo software

Il fornitore deve garantire quanto segue:

41. **Ciclo di vita di sviluppo software**:
    41.1. Deve essere predisposto un framework di sviluppo di software e sistemi riconosciuto.
    41.2. I sistemi e le applicazioni devono essere sviluppati seguendo le best practice di sviluppo di software sicuro (OWASP).
    41.3. Il codice del software deve essere:
        41.3.1. Protetto da modifiche non autorizzate
        41.3.2. Conservato in sicurezza
        41.3.3. Soggetto a processi di controllo della qualità
    41.4. Devono essere eseguite revisioni del codice.

42. **Test e distribuzione**:
    42.1. Le applicazioni devono essere sottoposte a test della sicurezza e della funzionalità prima della distribuzione nell'ambiente di produzione.
    42.2. Gli ambienti di produzione e non produzione devono essere adeguatamente separati.

42.3. La separazione delle funzioni fra lo sviluppo in produzione e non in produzione deve essere garantita.
42.4. I dati di produzione non devono esistere in un ambiente di test.

Sicurezza delle applicazioni

Il fornitore deve garantire quanto segue:

43. Sicurezza delle applicazioni:

43.1. Le verifiche della sicurezza delle applicazioni vengono condotte per le applicazioni di nuovo sviluppo e per tutte le applicazioni esistenti sottoposte a modifiche significative per identificare le vulnerabilità della sicurezza note.
43.2. Tutte le vulnerabilità della sicurezza identificate con un punteggio CVSS superiore a 4 devono essere neutralizzate prima di distribuire l'applicazione nell'ambiente di produzione.
43.3. I processi di revisione del codice vengono implementati per identificare e correggere codici che possono introdurre vulnerabilità della sicurezza.

44. Protezione delle applicazioni web:

44.1. Le applicazioni web rivolte al pubblico sono protette tramite un solido firewall dell'applicazione web per prevenire minacce esterne.

Gestione delle patch

Il fornitore deve garantire quanto segue:

45. Sono applicate le patch di sicurezza più recenti ai sistemi, alle reti, alle applicazioni e ai database in maniera tempestiva e in base alla criticità della vulnerabilità cui si riferisce la patch. Le patch sono fornite dai rispettivi OEM direttamente per i sistemi proprietari.
46. Tutte le patch sono state testate prima di essere distribuite ai sistemi di produzione ed è stato verificato il corretto funzionamento del servizio dopo l'attività di applicazione delle patch.
47. Sono disponibili misure di mitigazione appropriate qualora non sia possibile applicare una patch a un sistema e l'efficacia di tali misure è valutata periodicamente, conservando le relative prove.

Protezione dai malware

Il fornitore deve garantire quanto segue:

48. Tutti i sistemi IT sono continuamente protetti da una soluzione di protezione dai malware che esamina i dati in entrata in tempo reale per prevenire interruzioni del servizio o violazioni alla sicurezza. Inoltre, devono essere adottate procedure di sensibilizzazione dell'utente adeguate. Il sistema anti-malware rileva varie minacce, fra cui, ma non in modo esaustivo, virus, spyware, worm, codici mobili non autorizzati, keyloggers, botnets e trojan.
49. Le firme malware vengono aggiornate regolarmente per garantire che i sistemi siano sempre dotati delle ultime definizioni delle minacce.
50. Il software di protezione dai malware è configurato per eseguire scansioni sia programmate che su richiesta e per isolare o eliminare qualsiasi file o software dannoso identificato.

51. Gli utenti finali non hanno i diritti o la capacità di disattivare la protezione antimalware.

Gestione delle vulnerabilità:

Il fornitore deve garantire quanto segue:

52. Processo di gestione delle vulnerabilità:

52.1. Politiche, processi e procedure riconosciuti per la gestione delle vulnerabilità completa.

52.2. Processi per ricevere, analizzare e gestire le vulnerabilità sia da fonti interne che esterne.

53. Valutazione delle vulnerabilità e rimedi:

53.1. Valutazioni delle vulnerabilità trimestrali sull'infrastruttura IT e le applicazioni del fornitore, inclusi i siti di disaster recovery.

53.2. Applicazione di rimedi per le vulnerabilità identificate con punteggio CVSS superiore a 4 entro le tempistiche stabilite.

54. Penetration test:

54.1. Penetration test annuali indipendenti sull'infrastruttura IT e le applicazioni del fornitore usati per i servizi di Alludo.

54.2. I test si propongono di identificare vulnerabilità sfruttabili e di prevenire le violazioni della sicurezza tramite attacchi informatici.

54.3. Alludo ha consentito l'accesso ai report dei penetration test/test di vulnerabilità rilevanti su ragionevole richiesta.

Creazione di registri e monitoraggio

Il fornitore deve garantire quanto segue:

55. I sistemi critici, incluse le applicazioni, sono configurati per generare registri degli eventi chiave (inclusi quelli degli accessi privilegiati e delle attività degli utenti) e per conservarli per un periodo minimo di 1 anno o secondo quanto stabilito dei requisiti normativi vigenti.

56. I registri degli eventi chiave (come appropriato) devono contenere almeno le seguenti informazioni:

56.1. Avvio e chiusura del sistema.

56.2. Stato di avvio e interruzione dei servizi e dei processi critici.

56.3. Modifiche nei parametri di configurazione, come modifiche nella configurazione di avvio del sistema.

56.4. Tentativi di accesso avvenuti correttamente e non riusciti.

56.5. Creazione, modifica e cancellazione degli account utente.

56.6. Sistema/risorse alle quali si è effettuato l'accesso.

56.7. Identificazione e posizionamento degli utenti che hanno effettuato l'accesso alle risorse e da dove.

56.8. Date e orario.

57. I registri di controllo sono raccolti e collegati da più fonti e sensori e archiviati in sicurezza e sono inalterabili, per consentire la ricostruzione degli eventi.

58. I processi di monitoraggio degli eventi di registro (preferibilmente in tempo reale) hanno lo scopo di rilevare le attività non autorizzate, gli obiettivi degli attacchi e garantire che i registri degli eventi siano esaminati.

Gestione degli incidenti

Il fornitore deve garantire quanto segue:

59. I ruoli e i processi sono chiaramente definiti per garantire una risposta pronta, efficace e organizzata agli incidenti riguardanti la sicurezza e la privacy delle informazioni.
60. I dipendenti e gli appaltatori vengono formati per riconoscere cosa rappresenta un incidente per la sicurezza e come e dove riportare qualsiasi incidente potenziale o confermato.
61. Il personale responsabile di analizzare gli incidenti e rispondervi è qualificato in questa materia e segue regolarmente le formazioni sulle pratiche di risposta efficaci agli incidenti.
62. Per tutti gli incidenti riportati è presente un repository con i dettagli delle azioni intraprese per mitigare l'impatto dell'incidente e le lezioni apprese dall'evento.
63. Alludo viene informata non appena l'azienda viene a conoscenza di eventuali incidenti relativi alla sicurezza che la riguardano entro 24 ore dal rilevamento.

Sicurezza fisica e ambientale

Il fornitore deve garantire quanto segue:

64. Sono implementate politiche e procedure per i controlli della sicurezza materiale e ambientali in linea con gli standard di settore.
65. Le strutture critiche che ospitano i sistemi IT, le applicazioni e il personale (data center, siti operativi) sono protetti da incidenti, attacchi e accesso non autorizzato.
66. Sono disponibili misure di sicurezza come controlli degli accessi elettronici, verifica dell'identità, guardie di sicurezza, gestione dei visitatori e monitoraggio tramite telecamere a circuito chiuso 24/7 per prevenire gli ingressi non autorizzati.
67. I video della sorveglianza sono conservati per almeno 30 giorni o per una durata maggiore se richiesto dalle disposizioni di legge.
68. L'accesso alle strutture è limitato al personale autorizzato per finalità specifiche e regolarmente verificato.
69. I visitatori sono accompagnati, i loro orari di ingresso e uscita vengono registrati e indossano sempre badge identificativi. Le schede o le chiavi di accesso vengono ritirate dopo la loro uscita.
70. Le strutture critiche sono protette da interruzioni della corrente elettrica grazie all'uso di gruppi di continuità o generatori per garantire il proseguimento delle operazioni.
71. Vengono condotte manutenzioni periodiche sui dispositivi critici come i generatori di continuità, i rilevatori di fumo, i sistemi antincendio e i sistemi di controllo degli accessi, conservando i registri.
72. Le strutture sono costruite con materiali ignifughi e dotate di allarmi antincendio, rilevatori di fumo, sensori di temperatura e allagamento ed estintori per proteggere da pericoli naturali.

73. Sono definiti meccanismi sicuri di smaltimento per i dati sia in formati cartacei che elettronici usando trituratori per la carta e metodi come la sanitizzazione, la smagnetizzazione o la distruzione per i supporti elettronici.

74. Una chiara politica per il mantenimento della scrivania garantisce un uso sicuro dei post-it, dei documenti scritti e dei supporti removibili.

75. L'efficacia dei controlli fisici e ambientali viene valutata almeno una volta all'anno.

Privacy e protezione dei dati

Se il fornitore o i suoi subincaricati del trattamento dei dati trattano i dati personali a nome di Alludo o dei clienti di Alludo, il fornitore deve garantire quanto segue:

76. Conformità alla normativa in materia di privacy e governance:

- 76.1. Rispettare tutte le leggi sulla protezione dei dati vigenti.
- 76.2. Stabilire un framework di gestione della privacy che include:
- 76.3. Politiche sulla privacy, informative, note e procedure (riviste annualmente).
- 76.4. Processi di gestione dei rischi e di governance della privacy.
- 76.5. Rispetto dei requisiti legali e normativi.
- 76.6. Tenere aggiornati i registri delle attività di trattamento dei dati di carattere personale di Alludo.
- 76.7. Definire e implementare ruoli e responsabilità appropriati per la privacy dei dati:
- 76.8. Nominare un responsabile della protezione dei dati (o equivalente).
- 76.9. Creare una funzione specializzata nella privacy dei dati.
- 76.10. Formare un comitato per coordinare le attività di conformità in materia di protezione dei dati.

77. Protezione dei dati e misure di sicurezza

- 77.1. Implementare misure di sicurezza standard di settore (ISO/IEC 27001:2013, SOC2, ecc.) per proteggere le informazioni di Alludo.
- 77.2. Applicare misure aggiuntive per i dati personali sensibili (crittografia, pseudonimizzazione).
- 77.3. Applicare controlli degli accessi:
- 77.4. Limitare l'accesso a seconda del bisogno e del principio del meno privilegiato.
- 77.5. Rimuovere prontamente i diritti di accesso in caso di licenziamento o di cambio di ruolo.
- 77.6. Condurre verifiche periodiche dei diritti di accesso.
- 77.7. Assicurare l'impegno alla riservatezza da parte di tutto il personale che tratta dati personali.

78. Gestione dei diritti dei soggetti interessati:

- 78.1. Assistere Alludo nel rispettare i propri obblighi in materia di diritti delle persone interessate.
- 78.2. Informare Alludo entro 2 giorni dal ricevimento di richieste da parte di persone interessate.

78.3. Rispondere alle richieste unicamente secondo le istruzioni di Alludo, salvo diversamente previsto dalla legge.

79. Risposta agli incidenti:

79.1. Informare Alludo entro 24 ore di violazioni dei dati personali che coinvolgono i dati di Alludo.

Misure per i subappalti

Il fornitore deve garantire quanto segue:

80. Sta conducendo valutazioni annuali dei rischi di terze parti su tutti i sub-responsabili del trattamento dei dati coinvolti nella gestione, elaborazione o archiviazione dei dati di Alludo. Tali valutazioni si propongono di valutare i controlli di sicurezza dei sub-responsabili del trattamento, le misure di protezione dei dati, la conformità alle normative pertinenti e la posizione di rischio complessiva. Su richiesta, i fornitori devono fornire la documentazione di queste valutazioni, affrontare tempestivamente eventuali rischi identificati e comunicare tempestivamente ai sub-responsabili eventuali modifiche o risultati significativi. Ci riserviamo il diritto di esaminare i risultati della valutazione e di richiedere ulteriori misure di sicurezza, se necessario.

Gestione continuità aziendale

Il fornitore deve garantire quanto segue:

81. È stata definita una politica di gestione della continuità operativa (BCM, Business Continuity Management), accompagnata da piani e procedure dettagliate. Questi documenti descrivono gli obiettivi di continuità aziendale dell'azienda e sono sottoposti a revisione e approvazione annuale.

82. Un framework di test BCM è sviluppato e implementato per valutare l'efficacia delle strategie di continuità aziendale esistenti.

83. Viene condotta un'analisi dell'impatto aziendale (BIA,Business Impact Analyses) almeno una volta all'anno o in seguito a modifiche organizzative importanti.

84. È stato stabilito un piano di gestione della crisi con specifiche disposizioni in caso di pandemia. Il piano assicura una risposta appropriata alle emergenze, focalizzandosi sulla tutela dei dipendenti, dei visitatori, dell'ambiente, delle risorse e mantenendo le operazioni aziendali critiche.

85. Il sistema BCMS viene sottoposto a un efficace test annuale, con rapporti dettagliati per ciascun test.

<End of Document>