SISTEMA DI GESTIONE INTEGRATO QUALITA', AMBIENTE E SICUREZZA DELLE INFORMAZIONI

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Classificazione: Documento pubblico

Sommario

1 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La Direzione di LASCAUX, consapevole dell'importanza e della necessità di avvalersi di un Sistema di Gestione per la Sicurezza delle Informazioni riconosciuto in ambito internazionale, al fine di garantire la qualità dei servizi forniti e perseguire la soddisfazione dei propri Clienti, ritiene opportuno rendere il proprio Sistema di Gestione Sicurezza delle Informazioni conforme allo standard **ISO/IEC 27001**, e agli standard **ISO/IEC 27017** e **27018**, con riferimento alle parti di servizio che prevedono erogazione di servizi cloud in modalità SaaS, e sottoporlo a audits periodici di Terza parte condotti da Enti di Certificazione accreditati.
È politica aziendale approvvigionare da aziende certificate 27001, 27017 e 27018 al fine di coprire la catena di fornitura in relazione ai servizi di sicurezza.

Il campo di Applicazione del Sistema di Gestione Integrato è il seguente:

"Sviluppo software per soluzioni informatiche su commissione e di proprietà. Consulenza e assistenza informatica alle organizzazioni. Erogazione di servizi cloud computing in modalità SAAS".

Obiettivi primari della presente politica di sicurezza delle informazioni aziendali sono i seguenti:

- Perseguire il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni come obiettivo strategico della Direzione;
- Stabilire obiettivi di Direzione in ambito Sicurezza delle informazioni e individuare adeguati KPI per la loro misurazione;
- Assegnare la responsabilità di tenuta sotto controllo degli asset aziendali al personale in modo che tutti, nelle modalità pertinenti al proprio ruolo e funzione, siano coinvolti e partecipi nella di-fesa del patrimonio delle informazioni aziendali;
- Garantire adeguato apprendimento di concetti, responsabilità, metodologie di prevenzione e risposta in ambito di Sicurezza delle informazioni attraverso programmi periodici di formazione;
- Stabilire modalità di controllo per il trasferimento all'esterno di asset aziendali;
- Assicurare che nell'alienazione di qualunque asset aziendale non si verifichi perdita in termini di riservatezza delle informazioni eventualmente in esso contenute;
- Porre in essere tutte le azioni possibili al fine di preservare l'integrità, la disponibilità e la riservatezza di qualunque asset appartenente a LASCAUX;
- Controllare gli accessi dei visitatori negli uffici aziendali e tutti gli accessi a qualsivoglia informa-zione aziendale effettuata dal Personale o da terzi a vario titolo;
- Verificare che tutte le postazioni di lavoro abbiano accesso protetto da password periodicamente modificate;
- Definire e testare periodicamente procedure di back-up efficaci;
- Stabilire con i clienti e con i fornitori responsabilità reciproche nella gestione della sicurezza delle informazioni;
- Verificare periodicamente l'efficacia del piano di Business Continuity e Disaster Recovery;
- Garantire la comunicazione verso gli enti preposti nel caso di incidente che determini un data breach, data leak o la perdita di dati;
- Definire, comunicare e implementare politiche di gestione del personale e dei collaboratori mira-te a prevenire rischi alla gestione della sicurezza delle informazioni e ad una crescita continua delle competenze e della cultura tecnico-organizzativa nel Settore;
- Sviluppare e mettere a disposizione applicazioni informatiche (on Premise e SaaS) ideate e

progettate con una logica di prevenzione e protezione dei rischi alla sicurezza delle informazioni in relazione al Cliente

- Verificare periodicamente l'efficacia generale del Sistema di Sicurezza delle informazioni attra-verso lo svolgimento di audit periodici e riesami.

2 ALLEGATO - POLITICHE DI CYBERSECURITY (NIS2 - GV.PO-01)

Integrazione alla Nuova Polita per la Sicurezza delle informazioni
Ambito: a)–p) Allegato 1 NIS2

2.1. Scopo, principi e campo di applicazione

La presente sezione integra la Security Policy aziendale e definisce l'impostazione della politica per la gestione del rischio di cybersecurity, coerente con il contesto organizzativo, la strategia di cybersecurity e le priorità aziendali. Si applica a: personale dipendente e collaboratori, fornitori e terze parti rilevanti, infrastrutture IT/OT (se presenti), reti, sistemi informativi, dati, servizi cloud (SaaS/on premise), ambienti di sviluppo e produzione, sedi e strumenti di lavoro.
Principi guida: protezione di riservatezza, integrità e disponibilità (CIA); gestione basata sul rischio; difesa in profondità; minimizzazione dei privilegi; segregazione dei compiti; tracciabilità e accountability; approccio security-by-design e privacy-by-design; miglioramento continuo tramite misurazione e riesame.

2.2. Contesto organizzativo, strategia e comunicazione della politica

La Direzione definisce obiettivi e priorità di cybersecurity in coerenza con: (i) modello di business e servizi erogati; (ii) requisiti normativi e contrattuali; (iii) minacce e vulnerabilità rilevanti; (iv) dipendenze da fornitori e servizi cloud; (v) tolleranza al rischio (risk appetite). La politica è comunicata e applicata tramite: pubblicazione controllata su repository documentale, onboarding e formazione periodica, clausole contrattuali con fornitori e comunicazioni mirate alle funzioni interessate secondo il principio di necessità di conoscere (need-to-know).

2.3. Ruoli e responsabilità (ambito b)

Sono definiti e mantenuti ruoli, responsabilità, autorità e deleghe in materia di cybersecurity, includendo almeno:

- Fornitori/terze parti: rispettano requisiti contrattuali di sicurezza e collaborano su audit e incident response.
- Owner di processo/asset: classificano e proteggono gli asset di competenza, autorizzano accessi secondo need-to-know.
- HR: applica requisiti di affidabilità del personale, onboarding/offboarding e formazione.
- IT/Operations: implementano controlli tecnici (hardening, patching, logging, backup, rete), gestiscono configurazioni e cambiamenti.
- Responsabile della Sicurezza delle Informazioni/Cybersecurity (o figura equivalente): coordina il programma di sicurezza, mantiene il registro rischi cyber, supervisiona controlli e piani.
- Organi di amministrazione e direttivi: approvano la politica e il risk appetite; ricevono reporting periodico su rischi, KPI/KRI, incidenti e piani di trattamento.

2.4. Politica di gestione del rischio (ambito a)

LASCAUX adotta un processo strutturato di gestione del rischio di cybersecurity che comprende: identificazione, analisi, valutazione, trattamento, accettazione e monitoraggio. Il processo è documentato e integrato con il sistema di gestione sicurezza delle informazioni (es. ISO/IEC 27001) e con la gestione dei rischi aziendali:

- Rischio residuo e accettazione: formalizzata dalla Direzione secondo deleghe approvate.

- Piani di trattamento: misure tecniche/organizzative, responsabili, scadenze, budget e criteri di verifica efficacia.
- Registro rischi cyber: mantenuto e riesaminato almeno annualmente e in caso di cambiamenti significativi (nuovi servizi, fornitori, incidenti).
- Metodo: criteri di impatto e probabilità, livelli di rischio, soglie di accettabilità e criteri di priorità.

2.5. Affidabilità delle risorse umane (ambito c)

Sono adottate misure per ridurre il rischio derivante da errori, negligenza o comportamenti dolosi del personale:

- Offboarding: revoca accessi e restituzione asset entro tempi definiti, verifica di completamento.
- Obblighi disciplinari: regole di utilizzo accettabile degli strumenti, gestione violazioni e sanzioni.
- Gestione privilegi: concessione e revoca tempestiva degli accessi (joiner-mover-leaver), segregazione dei compiti.
- Selezione e onboarding: verifiche proporzionate al ruolo, sottoscrizione impegni di riservatezza e accettazione policy.

2.6. Conformità e audit di sicurezza (ambito d)

LASCAUX assicura la conformità a requisiti applicabili (normativi, contrattuali e di standard adottati) e svolge verifiche periodiche sull'efficacia dei controlli:

- Riesame della Direzione: almeno annuale con KPI/KRI, esiti audit, incidenti, stato piani.
- Audit di terza parte: supporto a verifiche di clienti/enti di certificazione e valutazioni indipendenti quando richiesto.
- Audit interni: pianificati almeno annualmente; gestione non conformità e azioni correttive.
- Mappatura requisiti: elenco requisiti applicabili e loro traduzione in controlli/ procedure.

2.7. Gestione dei rischi della catena di approvvigionamento (ambito e)

I rischi di cybersecurity legati a fornitori e terze parti sono gestiti lungo l'intero ciclo di vita della fornitura:

- Gestione fine contratto: restituzione/cancellazione dati, revoca accessi e verifica completamento.
- Monitoraggio: riesame periodico dei fornitori critici e controllo performance/sicurezza.
- Requisiti contrattuali: clausole su sicurezza, riservatezza, subfornitura, logging, notifica incidenti, diritto di audit, localizzazione dati.
- Due diligence e qualificazione: valutazione sicurezza del fornitore (questionari, evidenze, certificazioni, SLA).

2.8. Gestione degli asset (ambito f)

Sono identificati, inventariati e classificati gli asset informativi e tecnologici, definendo proprietà e regole di protezione.

- Protezione endpoint: requisiti minimi (antimalware/EDR, cifratura disco, patching, MDM se applicabile).
- Gestione ciclo di vita: acquisizione, assegnazione, manutenzione, sostituzione e dismissione sicura (sanitizzazione).
- Classificazione informazioni: livelli (es. pubblico, interno, riservato, critico) e regole di etichettatura/handling.

- Inventario asset: hardware, software, account, servizi cloud, repository codice, certificati, dati e informazioni.

2.9. Gestione delle vulnerabilità (ambito g)

Le vulnerabilità sono identificate e gestite con un processo strutturato che include rilevazione, valutazione, priorità e remediation.

- Eccezioni: approvate e documentate con rischio residuo e scadenza.
- Patch e remediation: finestre di manutenzione, mitigazioni temporanee, verifiche post-intervento.
- Valutazione: criticità (CVSS o equivalente), esposizione, impatto sul business e dipendenze.
- Fonti: scan periodici, monitoraggio bollettini, advisories vendor, segnalazioni interne/esterne.

2.10. Continuità operativa, disaster recovery e crisis management (ambito h)

Sono definite misure per garantire continuità dei servizi e gestione delle crisi informatiche:

- Crisis management: attivazione unità di crisi, comunicazioni interne/esterne, decisioni e post-incident review.
- Piano DR: procedure di ripristino, ruoli, contatti, checklist e prove periodiche.
- Backup: policy su frequenza, retention, cifratura, segregazione e test periodici di restore.
- BIA e scenari: identificazione servizi critici, RTO/RPO, dipendenze e priorità di ripristino.

2.11. Autenticazione, identità digitale e controllo accessi (ambito i)

Gli accessi a sistemi e dati sono gestiti secondo principi di minimo privilegio e need-to-know, con autenticazione forte dove applicabile.

- Policy password: complessità, rotazione dove necessario, protezione da riuso e da compromissione.
- Privileged Access: segregazione, session recording ove applicabile, vault/rotazione credenziali.
- MFA: obbligatoria per accessi amministrativi e accessi remoti/ cloud ove tecnicamente possibile.
- Gestione identità: account nominali, divieto di condivisione credenziali, revisione periodica degli accessi.

2.12. Sicurezza fisica (ambito j)

Sono adottate misure di sicurezza fisica per proteggere persone, locali, infrastrutture e asset:

- Smart working: regole per uso ambienti non controllati e protezione dei documenti.
- Gestione ambientale: alimentazione elettrica, UPS dove richiesto, protezioni base antincendio e condizioni operative.
- Protezione apparecchiature: posizionamento sicuro, blocco schermo, protezione da furti e manomissioni.
- Controllo accessi ai locali: badge/chiavi, registro visitatori, accompagnamento, limitazioni aree sensibili.

2.13. Formazione e consapevolezza (ambito k)

La Direzione promuove una cultura della cybersecurity tramite programmi di formazione, comunicazione e verifiche.

- Tracciamento: registri presenze, test di apprendimento e azioni correttive.

- Esercitazioni: simulazioni di phishing e tabletop exercise su incidenti e crisi.
- Formazione per ruoli: amministratori, sviluppatori, helpdesk, management (responsabilità NIS2).
- Formazione iniziale e periodica: phishing, gestione credenziali, uso strumenti, gestione dati e incident reporting.

2.14. Sicurezza dei dati (ambito l)

I dati aziendali e dei clienti sono protetti lungo il ciclo di vita con misure tecniche e organizzative proporzionate.

- Retention e cancellazione: tempi di conservazione definiti, cancellazione sicura e verificabile.
- Data loss prevention: controlli su esportazioni, condivisioni, supporti rimovibili e canali non autorizzati.
- Cifratura: in transito e a riposo dove applicabile; gestione sicura delle chiavi.
- Classificazione e minimizzazione: raccolta solo dati necessari e definizione responsabilità di trattamento.

2.15. Sviluppo, configurazione, manutenzione e dismissione (ambito m)

Per sistemi informativi e di rete si applicano requisiti di sicurezza lungo l'intero ciclo di vita, inclusi sviluppo software e gestione delle modifiche:

- Dismissione: revoca accessi, rimozione dati, distruzione/sanitizzazione supporti e aggiornamento inventari.
- Sicurezza applicativa: code review, gestione dipendenze, SAST/DAST ove applicabile, gestione segreti (secrets management).
- Hardening e configurazioni: baseline di sicurezza, gestione configurazioni e controllo modifiche (change management).
- Security-by-design: requisiti di sicurezza nei progetti, threat modeling proporzionato e review architetturali.

2.16. Protezione delle reti e delle comunicazioni (ambito n)

Le reti e le comunicazioni sono protette tramite segmentazione, controllo traffico, cifratura e configurazioni sicure:

- Gestione certificati e TLS: configurazioni aggiornate e deprecazione protocolli deboli.
- Sicurezza e-mail: filtri antispam/phishing, SPF/DKIM/DMARC ove applicabile.
- Perimetro: firewall, WAF dove applicabile, gestione sicura VPN e accessi remoti.
- Segmentazione: separazione ambienti (sviluppo/test/produzione), reti interne e servizi esposti.

2.17. Monitoraggio degli eventi di sicurezza (ambito o)

Sono attivati meccanismi di raccolta e analisi dei log e degli eventi di sicurezza, coerenti con i rischi e con i servizi erogati:

- Revisione: analisi periodica e verifica efficacia del monitoraggio.
- Alerting: soglie e correlazioni per eventi rilevanti; integrazione con ticketing/incident management.
- Conservazione log: tempi definiti, integrità e accessi controllati ai log.
- Logging: sistemi critici, amministrazioni, accessi, attività anomale e eventi di sicurezza.

2.18. Risposta agli incidenti e ripristino (ambito p)

LASCAUX mantiene un processo di gestione incidenti che copre rilevazione, analisi, contenimento, eradicazione, ripristino e lesson learned:

- Post-incident review: analisi causa radice, azioni correttive e aggiornamento controlli e formazione.
- Notifiche: obblighi verso clienti/autorità e canali di comunicazione; tracciamento decisioni e evidenze.
- Piano di risposta: ruoli, contatti, playbook per scenari comuni (phishing, ransomware, data breach, indisponibilità servizi).
- Classificazione incidenti: livelli di gravità, criteri di escalation e tempi di risposta.

3 APPROVAZIONE, APPLICAZIONE E RIESAME DELLA POLITICA

Le politiche per gli ambiti a)–p) sono approvate dagli organi di amministrazione e direttivi. La loro diffusione è garantita alle articolazioni competenti secondo need-to-know. Il riesame è almeno annuale e ogniqualvolta intervengano cambiamenti significativi o incidenti rilevanti.

Tutto il Personale, i collaboratori, i fornitori, i visitatori, dovranno operare nel rispetto delle norme e delle procedure aziendali predisposte al fine di assicurare la gestione del business aziendale in conformità ai predetti principi.

La Direzione si augura di ottenere, a tutti i livelli, la massima collaborazione per il rispetto e la sistematica applicazione di tali linee di indirizzo generali. Allo scopo ha definito, comunicato e rese consapevoli le persone che operano sotto il suo controllo sulle responsabilità, le autorità, le procedure e le istruzioni a più livelli in relazione ai ruoli ricoperti.

Il Direttore Generale

GIUSEPPE BISTONI