THM - SGI - Politica per la qualità e la sicurezza delle informazioni v2 del 08/2025 (Estratto)

Al fine di affermare il proprio impegno verso il mercato e verso le autorità di vigilanza e tutela nel campo della cybersicurezza nazionale e con l'obiettivo di garantire un'efficace gestione della sicurezza delle informazioni e della qualità, Themis ha deciso di definire ed implementare un sistema integrato per la gestione della qualità e della sicurezza delle informazioni (in breve, SGI) in conformità alle norme ISO 9001 e ISO/IEC 27001, con i controlli estesi sulla base delle norme ISO/IEC 27017 e ISO/IEC 27018, nel rispetto, infine, di quanto previsto dal Regolamento UE 2016/679 (di seguito GDPR).

Di fatto, l'adozione di un SGI rappresenta una decisione strategica per l'organizzazione e vuole essere una dimostrazione della volontà di porsi formalmente in un'ottica di miglioramento continuo e di focalizzare le proprie attenzioni alla sicurezza e alla qualità dei servizi forniti ai propri clienti.

La presente politica, dunque, definisce gli obiettivi, i principi guida, i ruoli e le responsabilità necessari all'implementazione di suddetto sistema.

Va segnalato inoltre che, tutte le politiche e le procedure che compongono il framework documentale a supporto del SGI referenziano e dipendono direttamente dalla presente politica.

La presente politica sarà oggetto di riesame periodico e di eventuale successivo aggiornamento almeno annuale, al fine di garantire costantemente una corretta rappresentazione della situazione aziendale.

1. **Scopo e ambito del documento**

Il presente documento ha lo scopo di definire i principi guida in materia di qualità e sicurezza delle informazioni, in conformità alle norme ISO 9001 e ISO/IEC 27001, con i controlli estesi sulla base delle norme ISO/IEC 27017 e ISO/IEC 27018, e le linee di indirizzo da considerare per garantire il corretto funzionamento del SGI, al fine di poterli comunicare in maniera ottimale sia all'interno di Themis che verso i soggetti esterni rilevanti.

L'ambito su cui insiste il SGI definito da Themis è formalizzato come: "Progettazione e gestione del servizio cloud Open Virtual Lab (OVL) per l'interconnessione dei dispositivi dei clienti ai servizi richiesti mediante la creazioni di reti virtuali private sicure".

La definizione di questo campo di applicazione, dettagliato in termini di asset nell'ambito delle attività di gestione del rischio IT, tiene in considerazione gli elementi definiti nei seguenti paragrafi.

2. **Contesto**

Fondata nell'anno 2004, grazie all'incubatore dell'università italiana del Politecnico di Torino, Themis S.r.l. (in seguito Themis) nasce come evoluzione di realtà professionali e societarie aventi come filo conduttore l'attività d'ingegneria del software.

Fin dalla sua nascita, Themis interviene nell'organizzazione e management di progetti per l'automazione di sistemi complessi, su specifiche che non hanno riscontro in soluzioni pronte nel settore IT, e nella raccolta, distribuzione e gestione di dati e condivisione delle risorse, integrando i

propri prodotti con le tecnologie più innovative che utilizzano il cloud come naturale centro nodale delle proprie piattaforme.

In questo contesto è stato progettato e sviluppato il servizio OVL: per fornire ai propri clienti un’innovativa piattaforma cloud che consente di creare una rete virtuale, in cui i sistemi e i software gestionali di tutte le strutture collegate sono a disposizione, senza limiti, del personale autorizzato all’accesso.

Themis ha determinato i fattori interni ed esterni rilevanti per il suo ambito, che influenzano (o possono influenzare) la sua capacità di raggiungere i risultati previsti dal suo SGI, come descritti di seguito.

Fattori interni:

- Cultura dell’organizzazione: La cultura orientata alla qualità e alla sicurezza delle informazioni di Themis costituisce un elemento favorevole all'implementazione di un SGI con il relativo insieme di politiche e procedure, che è in continua crescita.
- Politiche, obiettivi e strategie per raggiungerli: Politiche, procedure ed obiettivi rientrano nella cultura di Themis e il suo personale li sta seguendo. Gli obiettivi di qualità e sicurezza delle informazioni sono noti e utilizzati e sono stati inclusi nella presente politica.
- Standard, linee guida e modelli adottati dall’organizzazione: Themis ha stabilito una serie di norme di qualità e sicurezza delle informazioni che toccano diversi argomenti chiave.
- Relazioni contrattuali: I contratti con i fornitori, i prestatori di servizi e i partner commerciali sono controllati e vengono monitorati anche riguardo l’ambito della qualità e della sicurezza delle informazioni.
- Processi e procedure: Le attività di sviluppo dei progetti possono avere requisiti relativi a qualità e sicurezza delle informazioni applicabili.
- Risorse e conoscenze: Sono allocate risorse specifiche relative alla qualità e alla sicurezza delle informazioni, come riportato nella presente politica.
- Audit precedenti o risultati di precedenti attività di risk assessment: La precedente attività di risk assessment sull'ambito descrive una situazione in crescita che necessita di perfezionamenti, in alcuni casi fondamentali per migliorare la postura di Themis in materia di qualità e sicurezza delle informazioni; è prevista una serie di azioni di trattamento coerenti.
- Dimensioni contenute dell’organizzazione: Le dimensioni contenute dell’organizzazione, con una relativa tendenza a non lavorare in modo strettamente proceduralizzato, abilitano da un lato una buona flessibilità mentre dall’altro possono essere limitanti in ottica di miglioramento continuo.

Fattori esterni:

- Sociali e culturali: Esiste una tendenza al "lavoro creativo" diffusa nei paesi dell'Europa meridionale, che è contraria all'istituzione e all'uso di procedure formalizzate.
- Politico, legale, normativo e regolamentare: Non ci sono questioni politiche, legali, normative o regolamentari eccezionali che influenzano la qualità e la sicurezza delle

informazioni di Themis, a parte le leggi applicabili elencate nella presente politica al paragrafo 1.4, e i rapporti contrattuali con i fornitori e i partner commerciali.

- Finanziari ed economici: La situazione finanziaria di Themis e le prospettive del settore sono in condizioni stabili-positive.
- Tecnologici: Le vulnerabilità del software e del firmware applicabili anche alle tecnologie di Themis e degli altri attori del mercato sono in aumento, influenzando tutti i tipi di asset ICT.
- Sistemi informativi, flussi di informazioni e processi decisionali: I sistemi informativi sono ospitati presso Cloud Service Provider certificati ISO/IEC 27001, il che permette di avvalersi di un ambiente sicuro per l'erogazione dei servizi.
- Competitivi: I concorrenti e i criminali informatici stanno aumentando le loro capacità di sicurezza informatica, non interessando però attualmente Themis.

Nell'ambito del SGI di Themis, le parti interessate, interne ed esterne, sono principalmente:

1. la struttura interna di gestione e progettazione del servizio;
2. i fornitori, le aziende e i professionisti esterni che forniscono prodotti e risorse utilizzate per le attività di sviluppo;
3. gli estensori dei riferimenti normativi e di legge applicabili, elencati nel presente documento, che comprendono norme internazionali in ambito qualità, sicurezza delle informazioni, protezione dei dati personali, sicurezza sul lavoro;
4. i partner commerciali che richiedono a Themis di fornire un'adeguata garanzia in materia di qualità e sicurezza delle informazioni;
5. l'Agenzia per la Cybersicurezza Nazionale (ACN) che richiede che i servizi iscritti sulla propria piattaforma Cloud Marketplace siano qualificati sia rispetto la qualità che la sicurezza delle informazioni;
6. il Consiglio di Amministrazione (CdA), che richiede di soddisfare le richieste dei clienti in ambito qualità e sicurezza delle informazioni e di ottenere la certificazione del SGI da utilizzare come vantaggio competitivo;
7. i Clienti di Themis a cui questa fornisce i propri servizi.

2. PRINCIPI GUIDA E OBIETTIVI PER LA QUALITA' E LA SICUREZZA

1. Principi guida

La presente politica individua i seguenti principi guida da perseguire nell'implementazione del SGI adottato da Themis:

ORIENTAMENTO AL CLIENTE

La fornitura di servizi di altissima qualità e pertanto anche sicuri a tutti i Clienti è la missione ultima dell'Organizzazione e deve essere sempre tenuta in massima considerazione nelle attività di tutti i giorni del personale.

RESPONSABILITÀ COLLETTIVA

La responsabilità per la qualità e la sicurezza delle informazioni è un impegno collettivo e non un'attività demandata a specifiche risorse: ne consegue che tutti i dipendenti ed i collaboratori, senza nessuna esclusione, devono contribuire a salvaguardare la sicurezza aziendale.

GARANZIA PER TUTTO IL CICLO DI VITA

La sicurezza delle informazioni e la qualità devono essere impostate e mantenute durante tutto il ciclo di vita del servizio, ivi incluse acquisizione, pianificazione, creazione, archiviazione, accesso, modifica, manutenzione, trasmissione, salvataggio e distruzione. Questo concetto va applicato in modo specifico alla progettazione, nell'ottica di ottenere dei prodotti o servizi sicuri e di qualità "by design" e già predisposti per essere operati al meglio "by default".

BILANCIAMENTO FRA RISCHI E CONTROMISURE

L'obiettivo delle contromisure non deve essere l'ottenimento di un irraggiungibile rischio IT nullo, bensì l'accurato e ponderato bilanciamento fra la valutazione dei rischi rilevati in un determinato ambito e il costo da sostenere per le relative contromisure. Quest'ultimo non deve superare quello dei rischi identificati.

MIGLIORAMENTO CONTINUO

La realtà aziendale si evolve continuamente per rispondere alle esigenze di business o al progresso tecnologico e ogni processo o attività può e deve essere migliorato in modo costante nel tempo. Combinando queste due considerazioni ne consegue che l'approccio da seguire deve essere ricondotto a un processo circolare, le cui fasi principali sono:

- Pianificazione di un'azione, miglioramento o soluzione;
- Esecuzione di tutte le attività legate all'azione;
- Valutazione dei risultati ottenuti e verifica di raggiungimento degli obiettivi;
- Controllo e misurazione dei risultati, finalizzato ad individuare nuovi punti di miglioramento e a verificare la bontà delle azioni intraprese.

La circolarità dell'approccio si realizza nel ritorno dall'ultimo punto citato al primo, contribuendo a creare un circolo virtuoso orientato al miglioramento continuo.

NEED-TO-KNOW E PRIVILEGI MINIMI

L'accesso alle informazioni aziendali deve essere autorizzato in modo da consentire la consultazione, la modifica, la trasmissione e la distribuzione delle informazioni ai soli soggetti che ne necessitano per lo svolgimento delle proprie mansioni lavorative, limitatamente all'intervallo temporale richiesto. Di conseguenza, i privilegi di accesso assegnati devono essere limitati al minimo indispensabile per svolgere le relative mansioni.

DIFESA MULTILIVELLO

Le minacce e le vulnerabilità possono insistere su diversi livelli di un'infrastruttura tecnologica, pertanto, all'atto del disegno e dell'implementazione delle misure di sicurezza deve essere sempre rispettato il principio della difesa multilivello (defense in depth), prevedendo differenti tipologie di protezione per ciascun livello architetturale.

SEPARAZIONE DEI RUOLI

L’assolvimento di operazioni critiche per la sicurezza delle informazioni o dei sistemi informativi a supporto deve sempre rispettare il principio della separazione dei ruoli (separation of duties), ovvero assicurando che un soggetto non si trovi mai nelle condizioni di completare un’operazione critica in completa autonomia. Per operazioni particolarmente critiche va previsto altresì il ricorso agli analoghi principi di segreto condiviso (split knowledge) e doppio controllo (dual control).

INEFFICACIA DELLA NON DIVULGAZIONE

L'adozione di soluzioni aperte, documentate e verificabili è sempre preferibile a quella di soluzioni proprietarie e segrete e un metodo di protezione non deve essere considerato tale solo perché il suo uso o le sue caratteristiche non sono note.

DOCUMENTAZIONE E COLLABORAZIONE

La scelta delle misure di sicurezza deve prevedere un processo decisionale documentato che dimostri la corretta implementazione dei requisiti di sicurezza.

2. **Obiettivi**

La presente politica individua gli obiettivi del SGI adottato da Themis in:

AMBITO DELLA SICUREZZA DELLE INFORMAZIONI:

1. minimizzazione del numero degli incidenti di sicurezza delle informazioni;
2. riduzione del livello di rischio IT determinato dal processo di IT risk assessment;
3. ottenimento e successivo mantenimento della certificazione ISO/IEC 27001, con i controlli estesi sulla base di ISO/IEC 27017 e ISO/IEC 27018.

AMBITO DELLA QUALITÀ:

1. miglioramento dell’efficienza dei processi di business aziendali;
2. miglioramento della soddisfazione dei clienti ed eventualmente degli utilizzatori;
3. ottenimento e successivo mantenimento della certificazione ISO 9001.

I sopracitati obiettivi sono soggetti a misurazione, controllo e riesame da parte dell’Alta Direzione con cadenza periodica, venendo fissati puntualmente ad ogni aggiornamento della presente politica.

Nei requisiti principali inerenti all’attività di sviluppo del software (indicati sia dalle parti interessate interne che da quelle esterne), vista la sensibilità del loro ambito d’impiego, sono incluse le caratteristiche di sicurezza degli applicativi sviluppati. I requisiti di sicurezza costituiscono pertanto parte integrante di quelli specificati per la gestione della qualità dei prodotti aziendali.