REPORT S3-L2

INTRODUZIONE

Nell'era digitale in cui le informazioni rappresentano un valore cruciale per le organizzazioni, la protezione dei dati sensibili degli utenti è diventata una priorità assoluta per l'Alta Direzione. Con il costante aumento delle minacce informatiche e l'evoluzione delle normative sulla privacy, garantire la sicurezza e la conformità dei dati è essenziale non solo per la salvaguardia dell'azienda, ma anche per preservare la fiducia dei clienti.

In risposta a questa esigenza, l'organizzazione ha deciso di adottare un approccio strategico basato sul framework COBIT, sviluppato dall'ISACA. Questo framework fornisce una guida esaustiva e strutturata per l'implementazione di controlli e processi volti a garantire la protezione dei dati sensibili, in conformità con le normative vigenti e al fine di promuovere la fiducia e la trasparenza nei confronti della clientela.

In questo contesto, il presente esercizio si propone di delineare le azioni necessarie per soddisfare le esigenze dell'Alta Direzione, concentrandosi specificamente sulla protezione dei dati sensibili degli utenti e sull'ottimizzazione della sicurezza informatica, senza trascurare gli impatti sull'affidabilità e sull'integrità dell'organizzazione.

Definizione degli Obiettivi

- **Enterprise Goal (EG)**: Il EG selezionato è EG02 - "Managed business risk", identificato come cruciale per garantire efficiente e sicura la gestione del rischio dei servizi aziendali.

- **Alignment Goal (AG)**: Per allineare l'obiettivo di ottimizzazione della fornitura dei servizi, si è scelto l'AG07 "Security of information" che mira a garantire che le politiche di sicurezza informatica siano in linea con gli obiettivi aziendali.

- **Governance and Management Objective (GMO)**: In linea con l'AG scelto, si è identificato il GMO (stabilire e mantenere politiche, standard e procedure di sicurezza informatica) che per questo scenario prevede l'utilizzo delle seguenti pratiche: EDM03, APO13, BAI10, DSS05, MEA02 e MEA04.

Selezione delle Pratiche

La pratica scelta per contribuire a soddisfare l'esigenza dell'Alta Direzione è:
APO13 (Managed security) → APO13.01- APO13.03

- APO13.01 (Stabilire e mantenere un sistema di gestione della sicurezza delle informazioni ISMS)
- APO13.02 (Definire e gestire un piano di trattamento del rischio sulla sicurezza delle informazioni)
- APO13.03 (Monitoraggio e review del piano ISMS)

Ruoli e Responsabilità

I ruoli e le responsabilità per la pratica scelta sono stati definiti secondo la documentazione del framework COBIT, in particolare la tabella RACI dove per ognu ruolo viene definito se esso sdia responsabile (R) o accauntable (A).

	Chief information security officer	Chief information officer	Head architect	Head development	Head IT operation	Head IT administrator	Information security manager	Privacy officer
APO13.01	**A**	**R**	**-**	**-**	**-**	**R**	**R**	**-**
APO13.02	**A**	**R**	**-**	**-**	**-**	**R**	**R**	**R**
APO13.03	**A**	**R**	**R**	**R**	**R**	**R**	**R**	**R**

Input/Output

Gli input e aoutput per le pratiche APO13 prevedono:

	INPUT	OUTPUT
APO13.01	Approccio alla sicurezza dell'organizzazione	• ISMS scopo • ISMS policy
APO13.02	• Lacune e modifiche necessarie per realizzare la capacità di destinazione • Descrizioni domini di base e definizione dell'architettura • Proposte di progetto per ridurre il rischio	• Piano di trattamento del rischio sulla sicurezza delle informazioni • Casi aziendali sulla sicurezza delle informazioni
APO13.03	Prioritizzazione e classificazione degli incidenti e dei servizi richiesti	• Raccomandazioni per migliorare ISMS • Rapporti degli audit sul ISMS

Documentazione Aziendale

La policy o la procedura relativa alla pratica dovrebbe essere descritta nel documento aziendale relativo alle politiche e privacy di sicurezza informatica, che stabilisce le direttive e le norme per garantire la protezione dei dati sensibili degli utenti.

Servizi, Infrastrutture e applicazioni coinvolte

Per questo scenario ed in base alle pratiche trattate vengono considerati i servizi:

- Servizi di sensibilizzazione alla sicurezza e alla privacy
- Servizi di valutazione della sicurezza da terze parti

Come applicazioni/tool verranno considerati i tool di gestione della configurazione.