

Politica Sulla Sicurezza Delle Informazioni

Il Sistema di gestione della sicurezza delle informazioni delle società del Gruppo Bakioglu Holding si basa sui seguenti principi fondamentali:

Affidabilità (riservatezza): impedire che le informazioni siano disponibili o accessibili a persone, entità o altri sistemi operativi non autorizzati

Integrità: garantire l'integrità e l'accuratezza delle risorse

Accessibilità: garantire l'accesso e la disponibilità su richiesta di una persona autorizzata

- Istituire, sviluppare e garantire la sostenibilità e il miglioramento continuo del sistema di gestione necessario per identificare, valutare e attuare i controlli relativi ai requisiti di sicurezza, ai rischi, alle vulnerabilità e alle opportunità in relazione alla nostra strategia aziendale e ai processi di sicurezza delle informazioni,
- Garantire il pieno rispetto dei requisiti legali, relativi alle attività e contrattuali, nonché la riservatezza, l'integrità e la disponibilità di tutte le informazioni archiviate su supporti fisici ed elettronici,
- Garantire il pieno rispetto di tutti i requisiti di legge in materia di normativa doganale,
- Definire i principi operativi per la gestione dei rischi, nonché sviluppare e attuare misure di controllo per i rischi legati alla sicurezza. Valutare costantemente le aspettative e gli sviluppi tecnologici per tenere sotto controllo i rischi,
- Ridurre l'impatto dei rischi legati alla sicurezza delle informazioni sulla continuità operativa e garantire la continuità operativa,
- Avere la capacità di reagire rapidamente a potenziali incidenti di sicurezza informatica e di mitigarne l'impatto,
- Ridurre al minimo i rischi legati alla sicurezza delle informazioni, sensibilizzare gli utenti e i dipendenti in materia di sicurezza delle informazioni e assicurarsi che siano ben consapevoli delle proprie responsabilità,
- Valutare le prestazioni in materia di sicurezza delle informazioni e l'efficacia del sistema di gestione della sicurezza delle informazioni rispetto agli obiettivi definiti,
- Garantire la protezione dei dati personali,
- Definire e valutare i requisiti di sicurezza dell'infrastruttura elettronica gestita, migliorarla adattandola agli sviluppi tecnologici e garantire la continuità del servizio,
- Garantire che i fornitori di servizi esterni rispettino i requisiti e le esigenze previsti dal sistema di sicurezza delle informazioni,
- Garantire un livello accettabile di sicurezza per l'accesso al sistema dall'esterno,
- Definire i requisiti di sicurezza delle informazioni di terze parti, clienti e fornitori e garantire che siano conformi al sistema di gestione della sicurezza delle informazioni,
- Tutelare e rafforzare la reputazione della Holding in caso di impatti negativi legati alla sicurezza delle informazioni,
- Definire gli standard di sicurezza informatica per le società del gruppo, verificarne l'applicazione a intervalli regolari e assicurarne il rispetto.
- Valutare i potenziali impatti dei cambiamenti climatici sulla sicurezza delle informazioni e mettere in atto le misure necessarie per mitigarli.