INDICE

REV	DATA	NATURA DELLA REVISIONE
00	24/09/2025	Prima emissione

REDATTO	VERIFICATO	APPROVATO
Ciervo Domenico - ICT	Attanasio Giulia, Lupi Valerio - QM, CIO	Guglielmi Andrea - SMI

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento descrive il Sistema di Gestione della Sicurezza delle Informazioni (ISMS) adottato da GESAC, in conformità al Regolamento Delegato (UE) 2022/1645 e la Direttiva UE 2022/2555 (NIS2).
Il sistema è strutturato per garantire la protezione dei dati, la gestione degli incidenti, la continuità operativa e il rispetto delle normative vigenti assicurando la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi ICT e dei processi aziendali critici.

L' ISMS è stato appositamente progettato per rispondere in modo integrato sia ai requisiti specifici del Regolamento Delegato (UE) 2022/1645 sia alle prescrizioni della Direttiva UE 2022/2555 (NIS2). Questa unicità garantisce che tutte le misure, le procedure e le strategie implementate da GESAC soddisfino contemporaneamente gli standard previsti da entrambi i riferimenti normativi, permettendo così una gestione della sicurezza allineata sia all'ambito aeronautico che a quello della sicurezza delle reti e dei sistemi informativi essenziali. In questo modo, la conformità agli obblighi di sicurezza previsti dalla NIS2 viene riconosciuta anche come adempimento dei requisiti stabiliti dal Regolamento 1645, assicurando coerenza e completezza nell'approccio alla sicurezza delle informazioni.

2. RIFERIMENTI

Leggi nazionali e sovranazionali	Regolamento UE n. 2016/679 (GDPR).	Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
	Direttiva UE 2022/2555 (NIS2)	Direttiva del parlamento europeo e del consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
	D. Lgs. n.101/2018	Codice in materia di protezione dei dati personali
	D. Lgs. n.138/2024	Recepimento della direttiva NIS2 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione
	Regolamento UE n. 2019/1583	Disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea, per quanto riguarda le misure di cybersecurity
	Regolamento UE n. 2018/1139	Requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea
	Regolamento Delegato UE n. 2022/1645	Modalità di applicazione del regolamento (UE) 2018/1139 del per quanto riguarda i requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea
Certificazioni	ISO 22301:2019	Gestione della Continuità Operativa
	ISO/IEC 27001:2022	Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni

Norme interne	GEN 007	Sicurezza informatica e data breach
	MN ICT 001	Manuale Metodologia Cyber Risk Assessment
	ICT 003	Airport ICT disruption
	ICT 004	Violazione dei dati personali
	ICT 008	Sicurezza Informatica: Gestione degli incidenti
	ICT 009	Sicurezza Informatica: Gestione degli accessi
	ICT 011	Verifica e monitoraggio delle terze parti

3. DEFINIZIONI

Attore di Minaccia: Possono essere individui, collettivi o entità e sono occasionalmente definiti come attori malevoli. Un attore di minaccia è un soggetto incaricato di cercare di infliggere danni a un'organizzazione.

Impatto: L'entità con cui il rischio, se realizzato, influirebbe sull'azienda riguardo al raggiungimento dei suoi obiettivi.

Vulnerabilità: difetto o una debolezza in un sistema, software, hardware o processo che un aggressore può sfruttare per ottenere un accesso non autorizzato, eseguire azioni dannose o compromettere la sicurezza di un sistema informatico.

4. RESPONSABILITA'

La gestione del ISMS è sotto la responsabilità del Cybersecurity & IT Compliance Manager.
E' sua responsabilità aggiornare l'ISMS secondo quanto descritto al paragrafo 6.

E' responsabilità del Chief Digital & Information Officer la supervisione strategica e l'implementazione delle tecnologie dell'informazione all'interno dell'organizzazione.

Il Direttore Sviluppo e Manutenzione Infrastrutture, in qualità di Stakeholder del Rischio & Business Continuity insieme al Cyber Security & IT Compliance Manager, svolge un ruolo centrale nel processo di valutazione del rischio di cybersecurity. Questo ruolo prevede che il Direttore riferisca direttamente agli organi di amministrazione e direzione dell'azienda, presentando loro le analisi e gli esiti relativi alla sicurezza informatica, e sia responsabile dell'approvazione delle politiche di sicurezza. In questo modo garantisce che le strategie e le decisioni in materia di sicurezza siano pienamente allineate agli indirizzi e agli obiettivi aziendali, assicurando una supervisione costante e un efficace coordinamento tra tutte le funzioni coinvolte.

5. DESCRIZIONE DEL PROCE SSO

Il Sistema di Gestione della Sicurezza delle Informazioni adottato da GESAC si fonda su un processo ciclico e strutturato, pensato per garantire una protezione continua e dinamica delle informazioni aziendali. Il processo si articola in diverse fasi: dalla definizione di politiche e obiettivi di sicurezza coerenti con la strategia aziendale, all'identificazione e classificazione degli asset informativi, passando per la valutazione e la gestione dei rischi associati. Vengono implementate misure tecniche e organizzative per mitigare le minacce e garantirne l'efficacia nel tempo, attraverso un monitoraggio costante e il riesame periodico dei controlli di sicurezza. L'ISMS promuove inoltre un approccio basato sul miglioramento continuo, supportato dalla formazione del personale, dalla gestione strutturata degli incidenti e dall'adeguamento tempestivo alle

evoluzioni normative e tecnologiche, assicurando così la resilienza dei processi aziendali e la tutela dei dati sensibili.

5.1 Sensibilizzazione e Cultura della Sicurezza

GESAC adotta una strategia interna e misure volte a migliorare la sensibilizzazione del personale e a promuovere una cultura della sicurezza attraverso una costante formazione multicanale (e-learning, simulazione attacchi phishing, comunicazioni).

5.2 Metodologia di Valutazione del Rischio

La metodologia di valutazione del rischio adottata da GESAC si articola in più fasi, in conformità al manuale MN ICT 001-METODOLOGIA CYBER RISK ASSESSMENT. Oltre all'identificazione degli asset e alla valutazione dell'impatto e della probabilità degli eventi, la metodologia prevede:

1) Il controllo delle circostanze che contribuiscono all'effettivo verificarsi dello scenario di minaccia, attraverso l'analisi degli attributi delle minacce e la correlazione con eventi storici e vulnerabilità note.
2) La riduzione delle conseguenze sulla sicurezza aerea associate al verificarsi dello scenario di minaccia, mediante l'adozione di misure di contenimento, piani di ripristino e azioni correttive definite nella procedura ICT 003-AIRPORT ICT DISRUPTION.
3) L'adozione di misure preventive per evitare i rischi, inclusa la definizione di controlli tecnici e organizzativi, la formazione del personale, e il monitoraggio continuo delle posture di sicurezza, come previsto dalla procedura GEN 007-SICUREZZA INFORMATICA E DATA BREACH.

5.3 Gestione degli Incidenti

La gestione degli incidenti di sicurezza informatica è disciplinata dalla procedura ICT 008-SICUREZZA INFORMATICA GESTIONE DEGLI INCIDENTI.
La gestione degli incidenti informatici rappresenta un pilastro fondamentale nella strategia di sicurezza di GESAC. In conformità con quanto stabilito dalla procedura ICT 008, il processo prevede una serie di azioni strutturate volte a garantire la tempestività e l'efficacia della risposta agli eventi che compromettono la sicurezza dei dati e dei sistemi critici. Ogni incidente informatico rilevato viene analizzato e classificato secondo la gravità, l'impatto sull'operatività e la tipologia delle informazioni coinvolte.
Uno degli aspetti centrali della procedura ICT 008 riguarda l'obbligo di notifica: in presenza di violazioni, anomalie o tentativi di accesso non autorizzato, il personale ha il dovere di segnalare prontamente l'evento ai referenti designati per la cibersicurezza. Tale segnalazione deve avvenire secondo modalità e tempistiche definite, consentendo l'attivazione immediata di azioni correttive e di contenimento. L'obbligo di notifica si estende anche ai casi in cui le violazioni riguardino dati personali o informazioni aeronautiche, facilitando la collaborazione tra le diverse funzioni aziendali e garantendo il rispetto delle normative vigenti.
In presenza di incidenti significativi, è previsto il coinvolgimento tempestivo delle autorità competenti, nonché la comunicazione formale agli enti esterni, secondo quanto previsto dalle disposizioni interne e dai regolamenti europei.
Attraverso questi meccanismi, GESAC si impegna non solo a mitigare l'impatto degli incidenti, ma anche a promuovere una cultura della responsabilità e della prevenzione, rafforzando la resilienza complessiva dell'infrastruttura ICT aziendale.
Il processo include la rilevazione, l'analisi, il contenimento, la risoluzione e il ripristino, nonché la comunicazione agli stakeholder e la revisione post-evento.

5.4 Gestione delle Violazioni dei Dati Personali

La procedura ICT 004 VIOLAZIONE DEI DATI PERSONALI definisce le linee guida per la gestione delle violazioni dei dati personali, in conformità al Regolamento UE 679/2016 (GDPR). Include la segnalazione, analisi, classificazione, risoluzione, investigazione post-evento, chiusura e notifica all'Autorità Garante e agli Interessati.

5.5 Norme di Utilizzo dei Sistemi Informatici

GESAC ha definito un processo formale attraverso la procedura aziendale GEN 007 che stabilisce le norme di utilizzo dei sistemi informatici. Tale procedura è finalizzata alla protezione dei dati e degli elementi del sistema informativo, e include le nozioni fondamentali relative a cosa sia un data breach e/o un incidente informatico. Inoltre, definisce ruoli e responsabilità in adempimento alle normative di legge.
Queste norme disciplinano una serie di comportamenti e pratiche che ogni persona autorizzata all'accesso deve adottare nello svolgimento delle proprie attività.
In particolare, gli ambiti di comportamento riguardano:

- Confidenzialità e protezione dei dati: È fondamentale mantenere la riservatezza delle informazioni trattate, evitando la divulgazione non autorizzata di dati personali, aziendali o sensibili e adottando tutte le misure necessarie per proteggerli da accessi indebiti.
- Utilizzo corretto delle credenziali: Le credenziali di accesso devono essere personali, uniche e non cedute a terzi. Chi accede ai sistemi ha l'obbligo di custodire con cura le password e di aggiornarle periodicamente, seguendo le indicazioni aziendali.
- Accesso alle risorse in base ai ruoli: Ogni persona può accedere esclusivamente alle risorse necessarie allo svolgimento delle proprie mansioni, secondo il principio del minimo privilegio. L'accesso a dati o applicativi non pertinenti al proprio ruolo è vietato.
- Utilizzo responsabile delle risorse IT: L'utilizzo delle apparecchiature, delle reti aziendali e dei software deve avvenire esclusivamente per scopi professionali e in modo conforme alle policy interne, evitando qualsiasi comportamento che possa compromettere la sicurezza o le prestazioni dei sistemi.
- Gestione delle segnalazioni: Ogni anomalia, sospetto di violazione, tentativo di phishing o accesso non autorizzato deve essere prontamente segnalato ai referenti per la cibersicurezza, in modo che possano essere attivate tempestivamente le necessarie azioni di contenimento e ripristino.
- Divieto di utilizzo improprio: È vietato installare software non autorizzati, utilizzare dispositivi privati non conformi, accedere a contenuti non legati all'attività lavorativa o compiere atti che possano generare rischi di sicurezza o danni all'immagine dell'organizzazione.
- Formazione e aggiornamento continuo: Chi utilizza i sistemi è tenuto a partecipare ai programmi di formazione e aggiornamento sulle tematiche di sicurezza informatica e protezione dei dati, per mantenere elevato il livello di consapevolezza e prevenire comportamenti a rischio.

Attraverso la definizione puntuale di questi ambiti comportamentali, le norme di utilizzo contribuiscono a creare un ambiente digitale sicuro, responsabile e conforme alle normative vigenti, rafforzando la resilienza complessiva dell'organizzazione contro i rischi informatici.

5.6 Continuità Operativa ICT

La procedura ICT 003 AIRPORT ICT DISRUPTION definisce le modalità operative da attuare in caso di disruption aeroportuale legata al fermo dei sistemi informativi. Include scenari di discontinuità, azioni di salvaguardia, gestione delle emergenze e protezione dei dati, in conformità agli standard ISO 22301 e ISO/IEC 27001.

5.7 Gestione dei Dati Aeronautici e delle Informazioni Aeronautiche

Nell'ambito del proprio sistema di gestione, il gestore aeroportuale utilizza sistemi che garantiscono la sicurezza dei dati operativi che riceve, produce o utilizza in altro modo. L'accesso a tali dati operativi è limitato solo a persone autorizzate, in possesso nulla osta di sicurezza. Sono adottati sistemi progettati per rilevare violazioni della sicurezza e allertare il personale deputato alla cibersicurezza, nonché strumenti per controllare gli effetti delle violazioni della sicurezza e per identificare azioni di ripristino e procedure di mitigazione per prevenirne il ripetersi (procedura ICT 008).

5.8 Gestione Accessi

Un elemento cardine per la protezione dell'infrastruttura ICT riguarda la gestione rigorosa degli accessi, regolamentata dalla procedura ICT 009. Questa disciplina definisce criteri, modalità e controlli per l'assegnazione, la modifica e la revoca dei diritti di accesso agli asset informatici aziendali, assicurando che ogni autorizzazione sia strettamente correlata ai ruoli e alle responsabilità operative delle persone autorizzate. La procedura dettaglia i flussi operativi per la richiesta di nuovi accessi, che devono essere sempre formalmente autorizzati, nonché i processi di revisione periodica dei privilegi esistenti al fine di rilevare ed eliminare eventuali discrepanze o accessi non più necessari.
Particolare attenzione è riservata ai meccanismi di autenticazione, che prevedono l'adozione di credenziali uniche, complesse e periodicamente aggiornate, oltre all'applicazione di sistemi di autenticazione a più fattori nei contesti più critici o sensibili. L'accesso viene costantemente monitorato, tracciato e registrato attraverso soluzioni di audit log, consentendo la rilevazione tempestiva di anomalie o tentativi di accesso non autorizzato.

5.9 Appalto delle Attività di Gestione della Sicurezza delle Informazioni

In riferimento alla parte IS.D.OR.235 del REGOLAMENTO DELEGATO (UE) 2022/1645, GESAC garantisce la gestione della sicurezza delle informazioni appaltate attraverso la procedura ICT 011 VERIFICA E MONITORAGGIO DELLE TERZE PARTI. Tale procedura definisce il processo di verifica, monitoraggio e gestione del rischio cyber dei fornitori e delle terze parti, con requisiti di sicurezza, criteri di valutazione, controllo degli accessi e gestione dei rapporti contrattuali.

5.10 Conservazione dei registri

GESAC assicura la conservazione, l'archiviazione e la tracciabilità dei registri relativi alle proprie attività di gestione della sicurezza delle informazioni, in conformità ai requisiti normativi applicabili. Vengono mantenuti registri puntuali riguardanti tutte le approvazioni ricevute e le valutazioni dei rischi effettuate, gli appalti delle attività di gestione della sicurezza, i processi principali individuati, le risultanze delle valutazioni dei rischi e le relative misure di mitigazione adottate. Inoltre, sono conservati i registri concernenti inconvenienti e vulnerabilità comunicati attraverso i sistemi di segnalazione ufficiali, nonché quelli relativi a eventi che potrebbero essere oggetto di rivalutazioni per individuare eventuali criticità non precedentemente rilevate. Tali registrazioni, custodite e gestite secondo procedure interne, garantiscono tracciabilità, trasparenza e supporto a ogni attività di audit, verifica o riesame delle misure di sicurezza adottate dall'impresa.

5.11 Gestione del cambiamento

Il presente documento è soggetto a revisione ogniqualvolta si verifichino mutamenti significativi nel quadro normativo di riferimento (es. aggiornamenti del Regolamento UE 2022/1645, Direttiva NIS2, normativa nazionale di recepimento), modifiche sostanziali nei processi ICT aziendali, o a seguito di audit di cybersecurity interni/esterni che ne evidenzino la necessità o ancora in caso di modifiche a sistemi ICT o all'introduzione di nuovi sistemi ICT secondo quanto previsto dalla procedura ICT006 SICUREZZA INFORMATICA-RICHIESTA MODIFICHE (CHANGE & PATCH MANAGEMENT) e in conformità a quanto stabilito dal Manuale di Aeroporto Parte B, sezione 2.2.10, garantendo la tracciabilità delle revisioni, l'approvazione da parte dei responsabili designati e la tempestiva comunicazione agli stakeholder coinvolti.

Si riportano a titolo esemplificativo alcuni casi di gestione del cambiamento:

- implementazioni/modifiche a sistemi ICT
- implementazione di nuovi processi volti ad una migliore gestione degli incidenti informatici;
- mutamenti degli obiettivi, politiche e procedure in materia di sicurezza delle informazioni in coerenza con la strategia aziendale;
- modifiche del quadro normativo vigente e degli standard di riferimento che portano all'obbligatoria modifica del processo di gestione;
- mutamenti a seguito della conduzione del risk assesment sugli aspetti di Cybersecurity.

L'owner del cambiamento definito nel Manuale di Aeroporto – ovvero il Process Owner nel caso ICT – ha la responsabilità di sincerarsi della necessità di informare preventivamente il Cybersecurity Manager affinché siano valutati gli impatti sulla sicurezza del processo supportato dal sistema ICT oggetto del cambiamento.

A seguito della valutazione, un riscontro sintetico sarà notificato agli owner coinvolti, i quali dovranno recepire le eventuali modifiche e osservazioni, al fine di salvaguardare la sicurezza e l'integrità del processo introdotto.

6. DIAGRAMMA DI FLUSSO

N/A

7. INDICATORI DI PRESTAZIONE

N/A

8. FORMAZIONE E INFORMAZIONE

L'informazione relativamente al presente Piano viene effettuata attraverso pubblicazione e reperibilità sul Portale Documenti.

9. LISTA DI DISTRIBUZIONE

Il presente Piano viene distribuito a tutti i soggetti interessati mediante pubblicazione sul Portale Documenti.

10. ALLEGATI

N/A