Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

Politica per la sicurezza delle Informazioni

CASINÒ SANREMO		**CSR-ALL-01**	
		Rev.	Data
		1.0	**26/02/2025**
Oggetto	**Politica per la sicurezza delle Informazioni**		
Redatto	Elisabetta Sanguineti		
Verificato	Marco Calvi		
Approvato	Gian Carlo Ghinamo		
Classificazione delle Informazioni	Uso Interno		

Storia del documento

Rev.	DATA	Creato da	Verificato da	Approvato da	DESCRIZIONE
1.0	26/02/2025	E. Sanguineti	M. Calvi	G.C. Ghinamo	Prima Emissione

Classificazione dei dati

Classificazione dei dati assegnata	Livello	Ambito di diffusione consentito
	Pubblico	Il documento può essere diffuso **all'esterno** dell'azienda.
X	**Uso interno**	Il documento può essere diffuso solo **all'interno** dell'azienda. È consentito darne comunicazione a terzi con clausola di non diffusione.
	Riservato	Il documento **può essere diffuso** all'interno dell'azienda. La sua visibilità è limitata ad un gruppo ristretto di persone. L'accesso al documento è soggetto a controllo. La divulgazione non autorizzata di tali informazioni riservate potrebbe compromettere la reputazione aziendale o esporre a pericolo persone fisiche. L'indicazione "Riservato" DEVE essere riportata anche nel Piè-di-pagina del documento.
	Strettamente Riservato	I dati o le informazioni strettamente riservati si caratterizzano per una diffusione circoscritta e destinata a un numero limitato di soggetti e sono rigorosamente disciplinati dal principio della necessità di sapere (è necessario sapere chi ne possiede copie e chi può accedervi). La divulgazione non autorizzata potrebbe recare un danno eccezionale all'azienda. Le informazioni strettamente riservate richiedono i controlli di sicurezza più severi e pertanto l'utente è tenuto a valutarne attentamente la natura.

Sommario

Elenco degli acronimi

ACL	Access Control List
ADM	Agenzia delle Accise, Dogane e dei Monopoli
ADS	Amministratore di Sistema
AC	Azione Correttiva
BC	Business Continuity
BCP	Business Continuity Plan
CEO	Chief Executive Officer
CDA	Consiglio di Amministrazione
DPO	Data Protection Officer
DIR	Direzione
DR	Disaster Recovery
DRP	Disaster Recovery Plan
GOSE	Ufficio Giochi on Line
GDPR	General Data Protection Regulation
GPG	Guardia Particolare Giurata
ICT	Information and Communication Technology
ISPC	Information Security, Privacy and Compliance
NAS	Network Attached Storage
NC	Non Conformità
PM	Piano di Miglioramento
RDIR	Rappresentante della Direzione
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RSC	Responsabile dei Sistemi di Controllo
RSGSI	Responsabile del Sistema di Gestione della Sicurezza delle Informazioni
RSQ	Responsabile del Sistema Qualità
RCO	Responsabile della Continuità Operativa
RTEC	Responsabile Tecnico
RGES	Responsabile di gestione
SAN	Storage Area Network
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
VRCO	Vice Responsabile della Continuità Operativa
VM	Virtual Machine

1. Scopo

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti dalla Divisione Giochi On-Line, in seguito chiamata GOSE, al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

Per GOSE la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione, al fine di garantire la continuità del business e minimizzare il rischio di danni, prevenendo incidenti di sicurezza e riducendo il loro potenziale impatto.

2. Ambito di applicazione

Il Sistema per la Gestione della Sicurezza delle Informazioni di **GOSE** si compone di persone, di processi e di tecnologie indispensabili per garantire che venga adottato un approccio basato sulla valutazione del rischio quando si considera l'implementazione dei controlli di sicurezza, la gestione della privacy e la continuità, tutti elementi necessari per supportare gli obiettivi aziendali.

Il SGSI è progettato per proteggere tutte le informazioni e le risorse di **GOSE** sia da minacce che da vulnerabilità, interne o esterne, intenzionali oppure accidentali.

È responsabilità di ogni persona a cui la presente politica è applicabile di trovarsi pienamente informato e aggiornato, tenendo sempre in riferimento l'ultima versione di ognuna delle politiche relative alla Information Security e Privacy ed i relativi processi applicabili in base ai ruoli assunti.

Il promotore esecutivo e responsabile della presente politica il RSGSI.

3. Perimetro di riferimento

GOSE è la divisione di Casino di Sanremo S.p.A. dedicata alla gestione speciale della raccolta del gioco a distanza in concessione della ADM di cui all'art. 1 comma 935 della Lg. 208 del 28/12/2015.

GOSE si occupa della gestione commerciale, amministrativa e tecnica della specifica concessione ottenuta da Casino di Sanremo S.p.A. registrata al num. 15044 rilasciata il 19/11/2019.
Il presente perimetro prende in considerazione solo le attività effettuate da GOSE che fa parte dell'area Giochi Tecnologici di Casinò di Sanremo S.p.A. come individuato dall'allegato organigramma ufficiale visibile anche sul sito istituzionale aziendale **https://www.casinosanremo.it/societa-trasparente**.
Per raggiungere lo scopo istituzionale del dipartimento, GOSE si avvale, per la componente tecnica e tecnologica, della collaborazione di qualificati fornitori esterni e, per l'attività di supporto alla propria gestione, degli uffici e servizi competenti di Casino di Sanremo S.p.A.; tutti i fornitori terzi agiscono su indicazioni dirette.
Nello specifico la piattaforma dei conti di gioco è stata affidata ad Exalogic S.r.L. – ente certificato ISO 27001 - che assume la piena responsabilità dal punto di vista tecnico e tecnologico fornendo adeguate livelli di sicurezza conformi alle regole dettata da ADM nella sopracitata concessione.
La componente sistemistica è gestita tramite server ospitati su cloud ARUBA anch'essa certificata ISO 27001.
I software relativi ai giochi sono forniti da qualificate società specializzate nel settore dei giochi on line e ospitate su specifici server residenti su server farm dislocate nello spazio economico europeo come da requisito previsto dalla concessione ADM di cui sopra.
L'elenco di fornitori e dei giochi offerti da GOSE sono indicati nel documento CSR-SGQ-P07.02 Elenco Fornitori Aziendali.
GOSE non effettua alcuno sviluppo software.
Le richieste di "change" relative alla piattaforma dei conti di gioco provenienti da ADM vengono inoltrate ai responsabili della piattaforma di gioco e da questi ultimi gestite; GOSE non entra in alcun modo nel processo di sviluppo delle richieste.

Il dipartimento GOSE è dislocato in una area riservata (Zona A) posta al piano seminterrato all'interno di una ulteriore area riservata non aperta al pubblico (Zona B) dedicata agli uffici amministrativi e direzionali dell'area dei Giochi Tecnologici, Stampa e Cultura a sua volta contenuta all'interno della stabile di Casino di Sanremo S.p.A. situato in Corso degli Inglesi,18 in Sanremo IM.

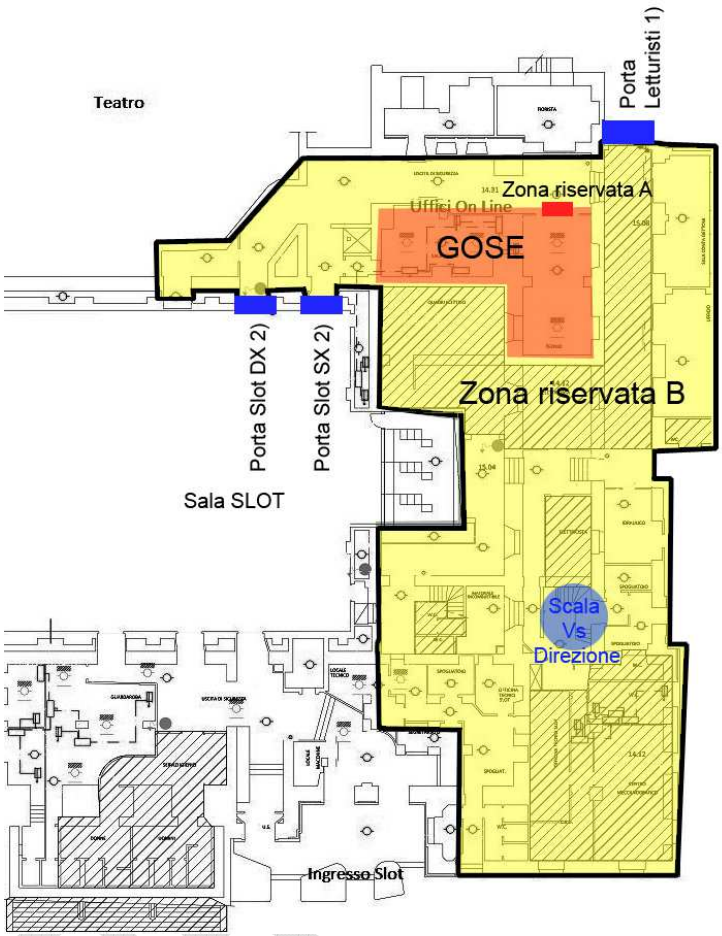

Fig. 1 – Raffigurazione planimetrica delle aree afferenti alla divisione GOSE

L'ufficio è uno spazio open con varchi di aereazione chiusi da griglie inferriate e dotato di unico accesso controllato da badge e da telecamere di sorveglianza poste esternamente all'ufficio, nell'area non aperta al pubblico.

La presente Politica per la sicurezza delle Informazioni (Information Security e Privacy Policy) si applica comunque a tutte le aree ed a tutto il personale GOSE, interno ed esterno, nello svolgimento di tutte le attività, che operino in sede o da remoto sia all'interno che all'esterno dell'azienda (es. smartworking o presso un fornitore), per dare evidenza al mercato di riferimento della capacità di erogare servizi oggetto della "mission" aziendale nel rispetto di tutti gli stakeholders che interagiscono con la società.

4. Politica

I nostri clienti si affidano ogni giorno alla nostra azienda e, per questo, abbiamo la responsabilità di gestire e proteggere le informazioni e le risorse dei nostri clienti nello stesso modo in cui proteggiamo le nostre.

A tal fine, la politica di sicurezza delle informazioni, approvata dal DIR, assicura che:

- Le informazioni saranno protette da qualsiasi **accesso non autorizzato;**
- La **riservatezza** delle informazioni sarà assicurata;
- L'**integrità** delle informazioni sarà mantenuta;
- Sarà mantenuta la **disponibilità** delle informazioni;
- Saranno soddisfatti i requisiti **legislativi e regolamentari**;
- Saranno sviluppati, mantenuti e testati **piani di continuità aziendale**;
- La **formazione sulla sicurezza delle informazioni** sarà disponibile per tutti i dipendenti;
- **Tutte le violazioni effettive e sospette della sicurezza delle informazioni** saranno segnalate al RSGSI e saranno oggetto di indagini approfondite.

GOSE implementa un sistema di gestione sicura delle informazioni attraverso:

- Procedure per sostenere la politica di sicurezza, comprese le misure di controllo dei malware, le password e i piani di continuità;
- Il soddisfacimento dei requisiti aziendali per la disponibilità di informazioni e dei sistemi;
- Il mantenimento della politica, del suo supporto, manutenzione e della consulenza durante la sua attuazione, che fa capo al RSGSI;
- La diretta responsabilità di tutti i manager dell'attuazione della politica e dell'assicurazione della conformità del personale nei loro rispettivi dipartimenti;
- L'obbligo per tutti del rispetto della politica di sicurezza delle informazioni.

4.1. Obiettivi della Politica

I seguenti obiettivi sono implementati a protezione delle informazioni, delle risorse e del personale di GOSE:

- Preservare l'attuale immagine dell'azienda quale player affidabile e competente;
- Proteggere il proprio patrimonio informativo sia fisico che culturale;
- Attuare la gestione delle informazioni per la protezione di tutte le informazioni;
- Assicurare la disponibilità e l'integrità dell'accesso a strutture, risorse e informazioni;

- Definire un programma di gestione della privacy progettato e implementato in conformità alla normativa del GDPR;
- Implementare una robusta continuità dell'organizzazione all'interno dell'azienda, con particolare precedenza per le attività, i sistemi e gli uffici strategici;
- Fornire consapevolezza ed erogare formazione in materia di sicurezza e privacy a tutto il personale, ivi compresi i propri consulenti e collaboratori;
- Fornire assistenza per la corretta attuazione dei requisiti e dei controlli per la gestione della sicurezza e della privacy;
- Condurre periodiche valutazioni dei rischi, dell'impatto sulla privacy e audit di conformità interni;
- Erogare una gestione coerente degli incidenti di sicurezza all'interno dell'intera organizzazione;
- Prevedere revisioni ed aggiornamenti annuali delle politiche, dei processi e delle attività in materia di sicurezza delle informazioni e della privacy.

Ciascuno degli obiettivi sopra elencati è disciplinato ed implementato in base ad una o più delle Politiche inerenti alla sicurezza delle informazioni e della privacy.

Per i motivi di cui sopra, GOSE ha deciso di intraprendere l'implementazione di un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

5. Responsabilità della Politica

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- Evoluzioni significative del business;
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- Significativi incidenti di sicurezza;
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

I dirigenti, i manager ed il gruppo che si occupa della gestione della Information Security, Privacy and Compliance (ISPC) assumono molto seriamente la responsabilità di garantire la sicurezza delle informazioni e sono fortemente impegnati per il mantenimento ed il miglioramento dell'SGSI come parte integrante della propria strategia aziendale.