Mercury S.p.A.
Società con socio unico
Via A. Manconi, 16 – 38122 Trento
Reg. Impr. Di Trento 02539960233
R.E.A.TN-227088 – Cap. soc. € 120.000 i.v.
C.F. e P.IVA 02539960233
Direzione e Coordinamento di Fingiama S.p.A.
mercuryspa.it

Sicurezza delle Informazioni

Policy per la Sicurezza delle Informazioni

Indice delle revisioni

Proprietario	Approvato da:	Classificazione
Persico – Peroni	CdA	Pubblico

Rev.	Motivo revisione	Autori revisione	Data revisione
00	Prima emissione	Persico - Peroni	5/08/2024

Mercury S.p.A.
Società con socio unico
Via A. Manconi, 16 – 38122 Trento
Reg. Impr. Di Trento 02539960233
R.E.A.TN-227088 – Cap. soc. € 120.000 i.v.
C.F. e P.IVA 02539960233
Direzione e Coordinamento di Fingiama S.p.A.
mercuryspa.it

Sommario

Introduzione

La politica di sicurezza delle informazioni stabilisce le basi e i princìpi cardine per la gestione dell'intero range di caratteristiche proprie del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) . La presente Policy rappresenta il principale strumento di comunicazione e condivisione delle direttive aziendali in materia di governo della Sicurezza IT, attraverso la definizione de:

- gli aspetti legali: linee guida per adempiere agli obblighi imposti dalle normative e dai regolamenti esterni a cui l'azienda si sottopone in materia di Sicurezza IT;
- l'impegno della gestione – *Governance:* principi e criteri generali di sicurezza che devono essere garantiti e rispettati nei processi;
- gli obiettivi di sicurezza;
- i ruoli e le responsabilità in relazione alla sicurezza delle informazioni.

Scopo

I principi generali declinati dalla presente Policy, che attengono a tematiche di Sicurezza Informatica e che trovano applicazione nelle modalità operative adottate dalla Società, hanno come obiettivo quello di salvaguardare il Sistema Informativo aziendale, assicurando che dati ed informazioni siano adeguatamente protetti, in conformità con i requisiti normativi in materia di protezione dei dati personali e di protezione degli asset aziendali.

Campo di Applicazione

La presente Policy è portata all'attenzione di tutto il personale dipendente e dei Fornitori/Outsourcer IT della Società al fine di garantirne il rispetto; pertanto, Mercury SpA si impegna a promuoverne la conoscenza, i relativi protocolli interni ed eventuali aggiornamenti tra tutti i lavoratori dipendenti ed i collaboratori che a loro volta dovranno conoscerne il contenuto, osservarlo e contribuire all'attuazione. Mercury SpA promuove altresì la conoscenza e l'osservanza della Policy anche tra gli outsources/fornitori, i partner commerciali, i consulenti, affinché seguano, nell'espletamento delle proprie attività, comportamenti volti ad aumentare il livello di sicurezza, di confidenzialità e di riservatezza delle informazioni trattate, nonché di prevenire il rischio di commissione dei reati contemplati nella normativa vigente.

Acronimi e abbreviazione

Nel documento sono utilizzati i seguenti acronimi:

- GDPR: General Data Protection Regulation
- CdA: Consiglio di Amministrazione
- DVR: Documento di Valutazione dei Rischi
- SGSI: Sistema di Gestione per la Sicurezza delle Informazioni

Ruoli e Responsabilità

Il settore IT chiama in causa tutti i ruoli d'azienda: fornendo gli strumenti per la quasi totalità dei lavori svolti, si ritrovano coinvolti nei processi informativi tutti gli utenti.

Nell'azienda ci sono figure e compiti dei responsabili e delegati alla gestione dell'intero sistema, come di seguito riassunto.

Il Consiglio di amministrazione ha la responsabilità di indirizzo e controllo del sistema informativo sul suo complesso e dunque approva:

- le sue strategie di sviluppo;
- la presente Policy di sicurezza informatica;
- l'adozione degli outsources/fornitori deputati a cui affidare la gestione del sistema informativo aziendale;
- le linee di indirizzo in materia di acquisizione di sistemi, software e servizi.

È imprescindibile che il CdA sia sempre informato in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo.

L'Amministratore Delegato ferma restando la responsabilità collettiva degli Organi Aziendali ha il compito di assicurare l'adeguatezza, la funzionalità e l'affidabilità del sistema informatico.

Il Responsabile IT (IT Manager) dell'azienda ha l'onere di supervisionare e gestire il dipartimento IT, includendo la pianificazione strategica delle tecnologie informatiche, la supervisione dei progetti e la gestione del team IT. Il Responsabile IT è il principale responsabile della sicurezza delle informazioni che garantisce il rispetto di tutte le politiche e le procedure di sicurezza, oltre ad essere l'interfaccia con l'Amministratore Delegato e gli organi aziendali che li aggiorna segnalando eventuali violazioni e criticità concernenti la sicurezza ICT.

Mercury SpA si avvale di diverse soluzioni in outsourcing e fornitori IT a cui ha affidato, diversi presìdi informatici. È pertinente ad ogni affidamento effettuato l'individuazione presso ogni outsourcer di una o più figure specifiche che tutelino e supportino Mercury SpA nel mantenimento e miglioramento degli standard di sicurezza anche tramite specifiche SLA ovvero tramite distintivi indicatori di performance.

Riferimenti Normativi

- ISO 27001:2022
- Articoli 24 e 24-bis del Decreto 231 del Codice Penale

I principi della Politica

I principi guida, trasversali a tutte le attività sensibili individuate, che fondano ed indirizzano l'approccio della Società Mercury SpA nei confronti della gestione della sicurezza informatica sono riconducibili ai seguenti criteri:

a) Segregazione delle attività: l'esercizio delle attività sensibili viene realizzato in osservanza del principio di segregazione tra chi esegue, chi controlla e chi autorizza.

b) Norme: la Società Mercury adotta e applica disposizioni organizzative idonee a fornire principi di riferimento generali per la regolamentazione dell'attività sensibile in conformità alla normativa emanata.

c) Poteri di firma e poteri autorizzativi: la società Mercury SpA ha formalizzato all'interno del corpo normativo l'elenco dei Responsabili muniti di poteri di firma e autorizzativi ed ha delimitato le competenze di coloro che svolgono fasi o attività cruciali di processi esposti al rischio.

d) Tracciabilità: i soggetti, le funzioni interessate e/o i sistemi informativi utilizzati, nel rispetto dei principi di tracciabilità e trasparenza delle operazioni effettuate, assicurano l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano la formazione e l'attuazione delle decisioni dell'organizzazione e le modalità di gestione delle risorse finanziarie.

e) Segnalazioni: nel caso in cui un esponente della Società riceva sollecitazioni - o ne venga a conoscenza anche per il tramite di terzi - ad effettuare attività in violazione delle regole procedimentali previste, quali negoziazione o stipulazione di contratti al di fuori dei limiti prestabiliti, lo stesso deve informare immediatamente l'AD o il Presidente (v. Codice Etico).

Parallelamente, l'approccio di Mercury riguardo la *governance* della sicurezza del dato richiama alle seguenti caratteristiche:

- riservatezza – protezione dei dati da modalità di fruizione non autorizzate (es: accesso ai dati da parte di soggetti non autorizzati, comunicazione di dati non autorizzata);
- integrità – protezione dei dati da attività volte alla loro modifica non autorizzata o indesiderata;
- disponibilità – protezione dei dati da possibili eventi in grado di ridurre la capacità dell'azienda di renderli disponibili (es. non raggiungibilità dei sistemi);

- conformità – gestione dei dati in modo conforme alle leggi ed alle normative in tema di sicurezza;
- verificabilità - la garanzia di poter ricostruire, all'occorrenza e anche a distanza di tempo, eventi connessi all'utilizzo del sistema informativo e al trattamento di dati;
- minimo privilegio – concetto di sicurezza in base al quale a ciascun utente siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati;
- segregazione dei compiti – il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite.

La pertinenza di tutti i criteri menzionati è estesa all'insieme di politiche, procedure e tecnologie utilizzate per proteggere i dati, la documentazione e gli asset logici, oltre a quegli accenni presenti anche nei servizi e personale, ovverosia gli ambiti di risorse così distinte nel documento di Politica Integrata.

Processi e procedure soggette a rischio.

Mercury SpA è in linea con il processo di analisi ed identificazione dei rischi intrinsechi all'attività aziendale, ma la cui corretta gestione preservare l'organizzazione e a generare valore nel lungo periodo.

A titolo esemplificativo, ma non esaustivo, si riportano alcune delle attività nel cui ambito potrebbero profilarsi dei reati in merito alla Sicurezza Informatica e sulle quali, dunque, è diretta la percezione dell'importanza dell'adozione della presente Policy; è opportuno segnalare che l'organizzazione non solo tratta dati per sé, ma erogando servizi ad altre società tramite specifici contratti di service può valutare le possibili compromissioni anche di questi ultimi.

- Gestione degli accessi al sistema informatico degli utenti interni ed esterni od operatori di sistema, dei profili utente e del processo di autenticazione.
- Gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni.
- Gestione della sicurezza fisica, ambientale (includendo apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni, intesi come asset fisici ed asset logici.
- Acquisizione e gestione, installazione o dismissione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione).
- Gestione degli aspetti infrastrutturali delle transazioni on-line.
- Gestione dei certificati digitali per la codifica delle comunicazioni o per la firma elettronica.
- Gestione del ciclo di vita delle applicazioni e delle richieste evolutive relative ad applicativi o al sistema informativo.
- Gestione delle procedure di elaborazione dei dati e la comunicazione/scambio di dati/accesso a piattaforme esterne di proprietà altrui.
- Gestione dello scambio delle informative verso le Autorità preposte alla vigilanza (ad es. flusso noleggio BT v. 26).
- Gestione degli adempimenti amministrativi, contabili e fiscali del ciclo attivo e del ciclo passivo (fatturazione, pagamenti, incasso, ecc.) inerenti all'operatività di competenza.
- Gestione dei procedimenti istruttori, delle segnalazioni ai fini antiterrorismo, delle attività di erogazione e delle connesse formalità amministrative relative alla concessione di finanziamenti

e/o garanzie ivi compresi quelli che godono di contributi e/o di garanzie pubblici riconducibili ai servizi gestiti in outsourcing.

- Gestione degli adempimenti informativi e delle anagrafiche nei confronti della clientela o degli uffici interni delle Società.

Obiettivi e azioni preventive

In risposta, ma soprattutto in un'ottica di impostazione di una policy efficace, Mercury intende formalizzare i seguenti obiettivi nell'ambito del SGSI:

- proteggere il proprio patrimonio informativo in modo che:
  - le informazioni siano protette da accessi non autorizzati tramite opportune politiche di accesso basate sui requisiti relativi alla sicurezza e all'attività dell'azienda;
  - le informazioni non vengano divulgate a personale non autorizzato a seguito di azioni deliberate o per incuria;
  - l'integrità delle informazioni sia protetta e salvaguardata da modifiche non autorizzate;
  - le risorse di supporto alle informazioni siano protette adeguatamente.

- Assicurare la protezione dei dati personali adempiendo agli obblighi dettati dal Regolamento Generale sulla Protezione dei Dati (GDPR) e la relativa normativa italiana attraverso:
  - l'elaborazione del registro delle attività di trattamento;
  - la valutazione di impatto sulla protezione dei dati, laddove applicabile;
  - l'applicazione di misure tecniche ed organizzative adeguate intese a garantire la sicurezza dei dati e assicurarne l'accountability e il rispetto dei principi di privacy by design e by default, in modo che i dati siano:
    - trattati in modo lecito, corretto e trasparente,
    - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità,
    - adeguati, pertinenti e non sovrabbondanti,
    - accurati e mantenuti aggiornati,
    - non conservati più a lungo del necessario,
    - trattati in conformità dei diritti dell'interessato,
    - sicuri,
    - non trasferiti all'estero senza adeguata protezione.

- Rispondere e reagire tempestivamente ad eventi che possano ridurre la sicurezza delle informazioni mediante:
  - redazione di procedure per la comunicazione tempestiva e per la gestione degli *incident* in caso di minaccia alla sicurezza dell'informazione, in modo che siano immediatamente individuabili i responsabili e le azioni correttive da intraprendere;
  - comunicazioni tempestive a chi di dovere relativamente a violazioni della sicurezza delle informazioni.

- Aumentare, nella propria organizzazione, il livello di sensibilità e la competenza sui temi di sicurezza attraverso:
  - comunicazioni aggiornate e adeguata formazione per tutto il personale, circa l'attuazione del SGSI;
  - programmi formativi di dettaglio sulla sicurezza delle informazioni per tutto il personale interno e per tutto il personale esterno che opera per periodi prolungati all'interno dell'azienda.

- Definire e mantenere sotto controllo, per quanto riguarda l'erogazione di servizi in modalità cloud:
  - le modalità di erogazione del servizio in cloud: SaaS, IaaS e PaaS;
  - la gestione degli accessi ai servizi erogati in modalità cloud, secondo il Regolamento Aziendale;
  - le comunicazioni ai customer in caso di *change* e agli interessati in caso di *data breach*;
  - il ciclo di vita degli account, definito nelle linee guida operative relative ai servizi erogati in modalità cloud;
  - il recepimento nell'analisi del rischio dei rischi aggiuntivi derivanti dall'erogazione di una infrastruttura cloud – l'analisi del rischio ISO/IEC 27001 viene effettuata includendo gli asset relativi ai servizi in cloud;
  - l'applicazione dei requisiti cogenti derivati dal Regolamento Europeo per la Protezione dei Dati Personal (GDPR).

Internal Audit

Gli internal Audit, schedulati e programmati seguendo un approccio *risk-based*, svolgono l'attività di revisione interna (c.d. "controlli di terzo livello") volta a garantire un'adeguata copertura delle varie applicazioni, infrastrutture e processi di gestione, ed in particolare le componenti esternalizzate. Inoltre,

valutano periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni.

Leadership e commitment

L'Alta Direzione di Mercury Spa, ponendo il Sistema Integrato per la Sicurezza delle Informazioni quale base strategica per il conseguimento degli obiettivi individuati, intende mostrare la propria leadership e il proprio impegno concreto.

Le principali azioni in tal senso sono:

COMMITMENT - SGSI	MODALITÀ DI ATTUAZIONE
Assicurare un'adeguata integrazione dei processi del SGSI nei processi dell'organizzazione	• Attività di formazione e consapevolezza • Attribuzione di adeguati ruoli, responsabilità e autorità.
Rendere disponibili adeguate risorse per il SGSI	• Azioni di mitigazione dei rischi • Piano di miglioramento del SGSI
Comunicare l'importanza dell'efficacia del SGSI e del conformarsi ai relativi requisiti	• Attività di formazione, consapevolezza, sensibilizzazione e responsabilizzazione di tutto il personale aziendale e delle eventuali terze parti coinvolte nei processi aziendali (consulenti, Fornitori, etc.).
Dirigere e supportare il personale nel contribuire all'efficacia del SGSI	• Attività di formazione e consapevolezza.
Promuovere il miglioramento continuo.	• Attività di formazione e consapevolezza • Piano di miglioramento del SGSI.
Supportare i responsabili di processo nel consolidamento della leadership nelle attività di loro pertinenza.	• Riunioni periodiche di pianificazione e comunicazione dei risultati

Outsourcer/Fornitori

In tutte le contrattualizzazioni stipulate, vengono sempre definite clausole contrattuali relative alla gestione delle misure di sicurezza delle informazioni; rafforzano anche la previsione di polizze assicurative e la formalizzazione di KPI, per il monitoraggio continuo delle implementazioni da parte dei fornitori.

A sostegno dell'effettivo rispetto delle misure di sicurezza sono prevedibili all'interno dei contratti specifiche attività di audit sulla terza parte, richiedendo formalmente la conformità a leggi e regolamenti – quale, ad esempio, la protezione dei dati.

È richiesto, a latere del costante monitoraggio svolto da Mercury SpA, a tutti gli Outsourcer/Fornitori di predisporre annualmente una specifica relazione sulla "Sicurezza Aziendale", da portare all'attenzione dei Vertici Aziendali e di Controllo.

Gli Outsourcer/Fornitori sono tenuti ad attenersi:

- ai principi e criteri generali di sicurezza che devono essere garantiti e rispettati nei processi di gestione della Sicurezza IT declinati nella presente Policy;
- alle linee guida per adempiere agli obblighi imposti dalle normative e dai regolamenti esterni a cui l'azienda si sottopone in materia di Sicurezza IT.

Diffusione

La Policy è portata all'attenzione di tutto il personale dipendente, degli outsourcers, dei fornitori IT di Mercury al fine di garantirne il rispetto.