Documento emesso il **18/12/2024** revisione numero **00**

A cura di EMILJAN KOLAJ. Approvato da MARCO SERMI

INDICE DELLE REVISIONI

N° Rev	Data Revisione	Emissione	Revisione	Approvazione	Descrizione Modifiche
0	18/12/2024	RSGSI *Emiljan Kolaj*	RSGSI *Emiljan Kolaj*	DIR *Marco Sermi*	Prima emissione

Sommario

Generalità

Sirius Technology s.r.l. (di seguito indicata come "Sirius") opera nel mondo delle telecomunicazioni.

Propone alla propria Clientela soluzioni complete comprensive di prodotti affermati a livello internazionale con i relativi servizi, e volte all'ottimizzazione dei processi trattati e all'innalzamento dell'efficienza aziendale. In tale ottica Sirius Technology si pone ai propri Clienti come partner attraverso la condivisione di obiettivi e opportunità, mantenendo come prioritario l'impegno all'imparzialità, alla trasparenza, alla riservatezza e alla competenza nei servizi erogati e nello sviluppo e attuazione del sistema di gestione della qualità conforme allo standard UNI EN ISO 9001

Sirius crede fortemente nel rinnovamento del settore ICT, adottando sistemi e tecnologie di ultima generazione sia per quanto riguarda gli applicativi, sia per quanto riguarda le infrastrutture hardware e di telecomunicazione.

Integrando le proprie capacità avanzate nella progettazione e realizzazione di sistemi di comunicazione con le più innovative tecnologie di elaborazione e comunicazione di dati ed informazioni, Sirius ha dato vita a soluzioni di supply chain affidabili, sofisticate ed innovative.

L'interconnessione tra le sedi è garantita da una infrastruttura di network bilanciata e ad alta affidabilità che garantisce uno scambio informativo in tempo reale.

L'integrazione lato sistemi applicativi consente di velocizzare l'acquisizione di dati fondamentali per approntare la progettazione, realizzazione e rilascio, ottenendo vantaggi consistenti sia sulla efficacia ed efficienza dell'erogazione, sia nel valore aggiunto dell'alta affidabilità garantita al Cliente sul piano della protezione dei suoi dati ed informazioni.

L'informazione è ritenuta pertanto un asset essenziale per il business di Sirius e come tale deve essere protetto.

Sulla base di tutte le motivazioni sopra riportate, l'Azienda considera fondamentale il miglioramento continuo delle performance di sicurezza delle informazioni nella conduzione dei propri processi gestionali, organizzativi ed operativi interni e lo ritiene uno strumento strategico attraverso il quale conseguire gli obiettivi del proprio business. A tal fine, ha stabilito di implementare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in accordo allo standard ISO/IEC 27001:2022, che risponda ai requisiti di sicurezza nell'ambito della progettazione ed erogazione di servizi integrati voce, dati, accesso internet, assistenza e supporto.

Il Sistema di Gestione per la Sicurezza per le Informazioni di Sirius individua e governa l'attuazione di un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- Riservatezza: proprietà dell'informazione di essere nota solo a chi ne è autorizzato;
- Integrità: proprietà di accuratezza dell'informazione e possibilità di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità: proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati

Al fine di fornire l'indirizzo generale e strategico nel breve, medio e lungo termine, per garantire la tutela e la protezione delle informazioni, nell'ambito delle proprie attività e in accordo con le indicazioni dello standard ISO/IEC 27001:2022, Sirius ha elaborato la sua politica in materia di protezione del patrimonio informativo aziendale, descritta in questo documento.

Indirizzo strategico e impegno della Direzione

Per raggiungere gli obiettivi di sicurezza delle informazioni individuati come necessari dalla Direzione aziendale, Sirius ha implementato un Sistema di Gestione della Sicurezza delle Informazioni coerente con la politica che l'azienda ha definito. Il mantenimento di tale sistema è garantito implementando un processo continuo di miglioramento continuo che coinvolga tutte parti interessate:

- Il personale, che mette in atto le politiche ed i requisiti di sicurezza per raggiungere gli obiettivi prefissati;
- Soci ed azionisti, che garantiscono la disponibilità delle risorse e la collaborazione nelle attività direzionali e organizzative;
- I partner operativi, che collaborano nelle attività di sviluppo e innovazione;
- I Clienti, cui è garantito il soddisfacimento delle esigenze di sicurezza, in misura conforme agli impegni assunti nei loro confronti;

- I fornitori, che contribuiscono al raggiungimento degli obiettivi dell'organizzazione, e accettano le politiche di sicurezza e le misure adottate per minimizzare i rischi connessi alla fornitura.

La Direzione è consapevole che l'implementazione del Sistema di Gestione richiede uno sforzo iniziale significativo e che il mantenimento e il miglioramento continuo devono essere garantiti da un supporto organizzativo adeguato.

A tale scopo, l'organizzazione di Sirius è strutturata in modo che i ruoli e le responsabilità sulla Sicurezza delle Informazioni siano definiti e siano in grado di operare nella direzione indicata dalla presente politica.

La Direzione rende disponibili gli investimenti idonei a soddisfare le politiche e gli obiettivi stabiliti e ritiene opportuno affrontare l'implementazione, il mantenimento e il processo di continuo miglioramento del proprio SGSI anche con l'inserimento di risorse esterne che siano in grado di dare il loro supporto qualitativo e quantitativo su tutti gli aspetti inerenti alla sicurezza delle informazioni.

Le attività previste per l'implementazione, il mantenimento e il miglioramento continuo del proprio SGSI sono effettuate da Sirius utilizzando:

- Risorse infrastrutturali ubicate presso Datacenter certificati TIER III e TIER IV;
- Risorse tecnologiche hardware e software a supporto delle attività operative;
- Risorse umane, consistenti nel personale di management e operativo della divisione IT aziendale, in relazione alle diverse competenze e ai ruoli assunti nel modello organizzativo implementato per il SGSI;

Il personale impiegato nelle attività operative, amministrative e contabili a supporto del core business, non direttamente coinvolto nella amministrazione e gestione dei sistemi informativi, è coinvolto nel raggiungimento degli obiettivi di sicurezza delle informazioni e rispetta tutte le indicazioni di gestione individuate dalla Direzione.

La governance del know-how e delle attività operative del personale è esercitata sotto il diretto controllo di Sirius.

Per tutte le attività e i servizi previsti per l'implementazione, il mantenimento e il miglioramento continuo del SGSI, è data garanzia della gestione sistemica delle seguenti attività, secondo i requisiti della norma ISO/IEC 27001:2022.

- **Governance**: attività che implica il controllo e la supervisione da parte di Sirius sulle politiche, le procedure e gli standard per la progettazione, la realizzazione, il collaudo, l'uso e il controllo dei sistemi informativi.
- **Conformità legislativa**: Sirius si assume la responsabilità di operare in accordo con le leggi stabilite, i regolamenti e le norme specifiche applicabili.
- **Affidabilità**: Sirius garantisce piena affidabilità relativamente al controllo diretto sugli aspetti di sicurezza e privacy assumendosi l'impegno di proteggere i sistemi informativi da operazioni non autorizzate di accesso, uso, comunicazione, interruzione, modifica, o distruzione, provenienti sia dall'esterno, sia dall'interno della struttura aziendale.
- **Competenza**: Sirius assicura che il personale coinvolto nelle attività incluse nel campo di applicazione sia in possesso dei requisiti di competenza, conoscenza e confidenzialità ai massimi livelli, garantendo un processo continuo di sensibilizzazione, istruzione, formazione ed addestramento, sia in ambito privacy e sicurezza delle informazioni, sia per quanto riguarda le competenze e qualifiche tecniche.
- **Controllo degli accessi ad aree ed edifici**: Sirius ha raggiunto un alto livello di sicurezza riguardo alla protezione delle aree, dei locali e degli uffici, installando sistemi di rilevazione e monitoraggio e sistemi di controllo accessi che mitigano i rischi legati a fattori ambientali, ad incidenti di natura fisica o ad azioni di danneggiamento volontarie ed involontarie.
- **Controllo degli accessi a sistemi e reti**: Sirius ha raggiunto un alto livello di sicurezza tramite l'applicazione di sistemi di autenticazione per l'accesso logico che garantiscono livelli minimi di rischio di accesso non autorizzato.

- **Accessibilità**: Sirius assicura l'utilizzo dei più efficienti sistemi per garantire la continuità operativa, il disaster recovery e l'accessibilità alle risorse informative.
- **Risposta immediata agli incidenti**: Sirius ha sviluppato procedure organizzative per far fronte alle conseguenze di eventi anomali ed incidenti che possano compromettere la sicurezza del sistema informativo. Sirius è consapevole che il ruolo assunto, anche nei confronti dei propri Clienti, è di vitale importanza nello svolgimento delle attività di risposta agli incidenti. Sono state predisposte modalità operative di segnalazione e intervento tempestivi, con l'ausilio di sistemi di logging e monitoraggio che coprono l'intero sistema.
-

Il patrimonio informativo aziendale

Qualunque tipo di dato o aggregazione di dati che hanno un valore per l'azienda, indipendentemente dalla forma e dalla tecnologia utilizzata per il loro trattamento e conservazione, contribuisce alla formazione del patrimonio informativo di Sirius. L'informazione deve essere protetta in tutti i possibili formati nei quali è resa disponibile:

- cartaceo (documenti, lettere, elenchi, etc.)
- elettronico (database, documenti digitali, immagini, video, etc.)
- verbale (riunioni, conversazioni personali e telefoniche, seminari, interviste, etc.)
- know how (competenze e conoscenza che contraddistinguono il personale di Sirius a tutti i livelli)

A seconda della tipologia e dell'origine, le informazioni che costituiscono il patrimonio Informativo aziendale possono essere suddivise in:

- Informazioni derivanti dal patrimonio informativo del Cliente, rappresentate dall'insieme delle informazioni gestite da Sirius nella erogazione dei servizi concordati. La sicurezza di queste informazioni è garantita per contratto, tenendo presente che qualsiasi incidente di sicurezza avrebbe conseguenze dirette sull'immagine e sullo sviluppo del business aziendale;
- Informazioni derivanti dal patrimonio informativo interno, rappresentate da tutte le informazioni interne all'azienda e gestite attraverso i sistemi ICT e non solo. Queste informazioni hanno influenza sulle altre e condizionano direttamente o indirettamente tutte le attività di business.

Le informazioni sono valutate per attribuire loro la relativa importanza a livello del business aziendale al fine di implementare contromisure di sicurezza adeguate e proporzionali alle diverse forme ed alle differenti modalità di interazione adoperate.

Valutazione dei rischi e quadro generale dei controlli

I requisiti di sicurezza sono identificati a mezzo di una valutazione sistematica dei rischi per la sicurezza delle informazioni, eseguita con metodologie validate da standard internazionali.

I risultati della valutazione dei rischi contribuiscono a determinare le azioni appropriate per la gestione e per l'implementazione dei controlli a protezione contro tali rischi, assegnando anche le relative priorità.

La valutazione dei rischi è ripetuta periodicamente e in caso si debbano affrontare eventuali cambiamenti che potrebbero influenzare i fattori di rischio.

I costi dei controlli la cui implementazione risulta necessaria a seguito dell'analisi dei rischi, vengono bilanciati dai benefici della protezione contro i danni che il business potrebbe riportare a causa di eventi inattesi o incidenti per la sicurezza delle informazioni.

Implementazione del Sistema e obiettivi

La presente politica di sicurezza delle informazioni individua gli aspetti di sicurezza da implementare all'interno dell'Organizzazione al fine di supportare la mission di Sirius e di perseguire i suoi obiettivi primari.

Gli obiettivi primari da perseguire secondo la politica di sicurezza delle informazioni adottata sono i seguenti:

- conformità alle normative cogenti
- monitoraggio e contenimento di rischi e minacce
- salvaguardia dell'immagine aziendale
- protezione del business
- rispetto degli accordi contrattuali
- mantenimento conformità allo standard ISO/IEC 27001:2022

Tali obiettivi possono essere raggiunti con l'impegno costante della divisione IT aziendale che provvede ad istituire il sistema di governo della sicurezza delle informazioni e con la collaborazione di tutte le strutture aziendali. Le strutture aziendali esterne al comparto IT, ciascuna per la parte di propria competenza, garantiscono l'applicazione di politiche e procedure volte a rendere Sirius capace di:

- garantire la riservatezza, l'integrità e la disponibilità delle informazioni;
- valutare i livelli di rischio;
- monitorare i livelli di sicurezza;
- formalizzare i requisiti di sicurezza in conformità alla normativa cogente e alle "best practices" del settore;
- garantire un adeguato livello di competenza del personale, raggiunto con la necessaria formazione e addestramento e con la trasmissione della consapevolezza dell'importanza della sicurezza delle informazioni;
- pianificare e gestire la continuità del business.

I contenuti delle indicazioni e delle prescrizioni del sistema si applicano a tutto il personale interno ed esterno, alle aziende partners, ai fornitori ed outsourcers ed a chiunque entri in contatto con le informazioni di proprietà di Sirius.

Tutto il personale che, a titolo di dipendente, consulente o collaboratore, collabora con Sirius nei processi di progettazione ed erogazione dei servizi e nel complesso dei processi di gestione organizzativa, contabile e amministrativa del business è responsabile dell'osservanza delle prescrizioni e delle indicazioni del sistema ed è tenuto a proteggere tutte le informazioni trattate durante le proprie attività lavorative. Il personale, consapevole dell'importanza delle informazioni trattate, deve agire per garantirne la protezione e provvedere alla segnalazione di anomalie di cui dovesse venire a conoscenza.

Nel caso in cui le regole di sicurezza stabilite siano disattese da dipendenti, consulenti e/o collaboratori, la Direzione di Sirius si riserva di adottare, nel pieno rispetto dei vincoli di legge e contrattuali, le misure più opportune nei confronti dei soggetti trasgressori.

I soggetti esterni che intrattengono rapporti con Sirius devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica, anche attraverso la sottoscrizione di un accordo di riservatezza all'atto del conferimento dell'incarico, nel caso in cui questo tipo di vincolo non sia espressamente citato nel contratto.

Conclusioni

Questa politica rappresenta gli obiettivi ed i requisiti generali emessi dalla Direzione di Sirius, che devono essere recepiti dalle strutture aziendali, ciascuna per lo specifico ambito di competenza, affinché l'attività lavorativa sia conforme ai principi evidenziati.

La Politica per la Sicurezza delle Informazioni deve essere sempre coerente con gli obiettivi di business aziendali e pertanto la Direzione si riserva di apportare eventuali modifiche al presente documento in base al conseguimento dei risultati di Sirius, alle aspettative di tutte le parti interessate e all'andamento del mercato di riferimento. Costituiscono motivo valido per il riesame e l'eventuale aggiornamento della presente politica i cambiamenti intervenuti nel corso del tempo trascorso dall'ultima revisione in tema di:

- strategie di business aziendale;
- ambiente tecnico e tecnologico;
- normative, regolamenti e contratti;
- rischi per la sicurezza delle informazioni;
- lesson learned ricavate dalla gestione di eventi ed incidenti di sicurezza delle informazioni.

In accordo alla Politica della Sicurezza delle Informazioni e con cadenza almeno annuale, la Direzione fisserà gli obiettivi per la sicurezza delle informazioni, ne verificherà il livello di raggiungimento e valuterà l'efficacia del proprio sistema di gestione sulla base del confronto con i risultati raggiunti nel corso dell'anno precedente.

Questa politica è stata approvata dalla Direzione Aziendale di Sirius Technology s.r.l..

Firma della direzione