POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Rev. 1.0

Versione	Data	Autore	Revisione	Approvazione Direzione
1.0	31/10/2023	Antonio Andrea Comandù	31/10/2023	23/11/2023

Leva
automotive interiors

Sommario

1. Distribuzione documentale

La distribuzione del presente documento è gestita da LEVA S.p.a. (di seguito anche LEVA) attraverso il sistema locale di distribuzione.

2. Scopo

Il Sistema di Gestione per la Sicurezza delle Informazioni (di seguito anche SGSI) definisce il livello di sicurezza che LEVA intende raggiungere nell'adempimento dei suoi compiti. Tale livello di sicurezza si basa su un insieme di requisiti essenziali per LEVA. La presente Politica sulla Sicurezza delle Informazioni, e le politiche e le procedure del SGSI in generale, contengono le indicazioni necessarie per implementare le strategie di Sicurezza delle Informazioni e per raggiungere gli obiettivi di Sicurezza delle Informazioni, attraverso un processo di miglioramento continuo definito secondo un approccio risk-based.

I concetti e le indicazioni sono formalizzati in politiche, procedure e altri documenti di supporto, e attuati mediante misure tecniche e organizzative, nonché processi di gestione per la Sicurezza delle Informazioni, integrati nel panorama dei processi già attivi di LEVA.

L'obiettivo della gestione della Sicurezza delle Informazioni è supportare e proteggere tutte le informazioni trattate nelle varie attività aziendali, per mezzo dell'infrastruttura tecnologica di LEVA.

La Politica sulla Sicurezza delle Informazioni (questo documento) contiene i principi fondamentali e i requisiti per la gestione di tutti gli aspetti inerenti alla Sicurezza delle Informazioni.

Queste regole, i processi applicati per la gestione della Sicurezza delle Informazioni, nonché le misure tecniche/organizzative implementate, costituiscono il SGSI di LEVA.

3. Politiche di sicurezza delle informazioni

La Sicurezza delle Informazioni è uno dei criteri di qualità più importanti in ambito ICT, insieme alla funzionalità e all'efficienza dei costi. L'insieme di tali criteri contribuisce al successo aziendale di LEVA e il corretto svolgimento delle sue attività commerciali.

La Sicurezza delle Informazioni protegge i diritti e gli interessi dei clienti, dei dipendenti, dei fornitori e di tutti i soggetti interessati (organizzazioni e individui) che interagiscono con LEVA.

L'innovazione e la gestione economica dei rischi sono requisiti importanti per l'individuazione, la valorizzazione e lo sfruttamento ottimale del potenziale commerciale. La Sicurezza delle Informazioni rappresenta un fattore critico per il successo aziendale: supporta attivamente l'innovazione in LEVA e pertanto costituisce un valore aggiunto e apporta un vantaggio competitivo.

LEVA riconosce che la necessità di Sicurezza delle Informazioni aumenta continuamente con l'incremento delle minacce dalla rete globale, i cambiamenti nei comportamenti d'uso e lo sviluppo di nuove tecnologie e funzionalità. Coerentemente, LEVA allinea la Sicurezza delle Informazioni agli standard internazionali nel rispetto dei requisiti stabiliti dalle normative cogenti e dei regolamenti applicabili.

Le risorse ICT devono essere utilizzate in modo sicuro e responsabile. Gli utenti delle risorse ICT conoscono i requisiti della Sicurezza delle Informazioni e li tengono in continua considerazione nel loro lavoro quotidiano.

Il comportamento di tutti i dipendenti di LEVA nei confronti degli aspetti legati alla Sicurezza delle Informazioni si basa sui seguenti principi:

- la Sicurezza delle Informazioni deve essere garantita in conformità con quanto previsto dal SGSI di LEVA.
- tutte le informazioni devono essere classificate secondo il SGSI fin dal momento della loro creazione.
- tutte le informazioni devono essere protette in base ai requisiti di protezione stabiliti.
- solo le persone chiaramente identificate con l'autorizzazione appropriata possono accedere alle strutture e alle informazioni.
- a seconda dello scopo aziendale, l'accesso alle informazioni deve essere limitato e documentato. Ciò potrebbe richiedere misure per identificare, tracciare e vincolare l'accesso a sistemi di memorizzazione, applicazioni, edifici, stanze e informazioni.

L'attuazione delle politiche di Sicurezza delle Informazioni richiede un elevato grado di consapevolezza sulla sicurezza. La Direzione promuove attivamente misure per sensibilizzare e formare i dipendenti su cosa significhi Sicurezza delle Informazioni per LEVA e i suoi clienti. La consapevolezza della sicurezza si caratterizza attraverso i seguenti comportamenti:

- una Sicurezza delle Informazioni efficace è un elemento essenziale della strategia aziendale di LEVA, e viene dimostrata attraverso la consapevolezza sulla sicurezza quale elemento presente e integrato in tutti i processi e le decisioni aziendali.
- identificando la responsabilità personale per garantire la Sicurezza delle Informazioni nell'operatività quotidiana del business, così come in caso di incidenti o situazioni di emergenza.

4. Obiettivi di Sicurezza delle Informazioni

Per implementare la strategia di Sicurezza delle Informazioni e raggiungere gli obiettivi di sicurezza, i processi aziendali e i prodotti devono essere adeguatamente protetti rispetto ai criteri di sicurezza - disponibilità, confidenzialità, integrità - e ai livelli di classificazione delle informazioni - definiti nel documento "LEVA - Politica Classificazione Informazioni v.1.0"

La confidenzialità comprende la protezione contro la divulgazione o l'accesso non autorizzato alle informazioni. I dati e le informazioni confidenziali sono accessibili solo alle persone autorizzate, in considerazione del loro ruolo e funzione secondo il principio del minimo privilegio e del "need to know".

La perdita di confidenzialità si verifica quando persone non autorizzate hanno acquisito conoscenza delle dette informazioni.

L'integrità si riferisce a garantire la correttezza delle informazioni e il corretto funzionamento privo di errori dei sistemi ICT. A seconda del contesto, le informazioni possono avere determinate attribuzioni come autore o tempo di creazione. La perdita dell'integrità delle informazioni si verifica quando le informazioni, le loro attribuzioni o entrambe sono state modificate senza autorizzazione.

La disponibilità di un sistema ICT, applicazione, rete o informazione significa che gli utenti possono usarli come previsto. La perdita di disponibilità si verifica quando l'uso previsto non è possibile per un certo periodo.

Le basi per gli obiettivi e le strategie di sicurezza si basano su aspetti legati a:

- Organizzazione (processi, ruoli e responsabilità) chiaramente definiti per garantire la Sicurezza delle Informazioni.
- definizione di strategie di Gestione del Rischio (Analisi del Rischio, livello accettabile di rischio residuo e accettazione del rischio).

- classificazione delle informazioni e delle risorse ICT (applicazioni aziendali e sistemi ICT).
- analisi delle minacce e il loro impatto sui processi aziendali e i conseguenti requisiti e necessità di protezione.
- Formalizzazione di principi per la pianificazione della continuità operativa aziendale, comprese le attività per garantire la sicurezza.

Un altro obiettivo strategico di LEVA è assicurare un processo di miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni, al fine di:

- garantire l'efficacia del SGSI.
- aumentare il livello di proattività (e la percezione di proattività da parte degli stakeholder) in merito alla Sicurezza delle Informazioni.
- rendere i processi e i controlli di Sicurezza delle Informazioni integrati ai processi di business misurabili al fine di garantire la valutazione della performance del SGSI e di fornire una base solida per decisioni informate.
- rivedere le metriche rilevanti su base annuale per valutare se è opportuno cambiarle, basandosi sui dati storici raccolti.

Il SGSI è allineato con le migliori pratiche standard; gli standard internazionali di sicurezza (ISO/IEC 27001:2022, 27002:2022, 27005:2022), per il SGSI, e i requisiti specifici per il settore automobilistico (TISAX).

5. Implementazione del SGSI

5.1. Informazioni generali

I processi di gestione della Sicurezza delle Informazioni supportano la progettazione e lo sviluppo del SGSI stesso. Definiscono il funzionamento e il supporto del SGSI, la gestione degli incidenti di sicurezza e la valutazione dei rischi per la sicurezza delle informazioni, secondo le politiche e le pratiche di LEVA.

Gli obiettivi di sicurezza e la strategia di sicurezza si applicano alle aree descritte nelle sezioni seguenti. A seconda dell'area, devono essere considerate ulteriori specifiche e politiche.

5.2. Struttura del SGSI

Il documento di alto livello è la Politica sulla Sicurezza delle Informazioni (questo documento), che ne definisce la strategia. Questa strategia viene concretizzata e mappata tramite le Politiche sulla Sicurezza delle Informazioni definite all'interno del SGSI.

La struttura delle aree di applicazione segue i requisiti di standardizzazione della norma ISO/IEC 27001:2022, che sono stati ampliati dai requisiti specifici del settore dei processi aziendali e dell'ambiente dei clienti di LEVA.

La tabella seguente mostra le singole politiche e procedure definite all'interno del set di documentazione del Sistema di Gestione della Sicurezza delle Informazioni e riepiloga il contenuto di ciascun documento e i metodi di pubblicazione.

Argomento	**Titolo del documento** *Sintesi del contenuto*
Riesame della Direzione Gestione delle Non Conformità e delle Azioni Correttive	*LEVA- Manuale della Qualità (Manuale Qualità IATF 06112017)* Documento che descrive, documenta, coordina e integra la struttura organizzativa di LEVA, e responsabilità e tutte le attività svolte.
Uso Accettabile dei beni aziendali	*LEVA - Regolamento Informatico Aziendale* Utilizzo accettabile dei sistemi informativi aziendali da parte di Dipendenti, Collaboratori e terzi autorizzati.
Contesto TISAX	*LEVA - Scopo del Sistema Gestione TISAX* Questo documento analizza l'ambito TISAX di LEVA. *LEVA - VDA ISA*
Classificazione delle Informazioni	*LEVA - Politica Classificazione Informazioni v.1.0* Descrive l'approccio metodologico di LEVA per classificare ed etichettare le informazioni.
Risk Management	*LEVA - Metodologia di Analisi dei Rischi_v.1.0* Descrive l'approccio metodologico per l'attività di Risk Management svolta da Gerico Security Srl per LEVA.
Mansionari	*Documenti vari* Documenti che descrivono ruoli e responsabilità assegnate all'interno dell'organizzazione di LEVA. *Organigramma Leva Group* Grafico che rappresenta i rapport gerarchici presenti all'interno dell'organizzazione di LEVA.
Audit	*LEVA - Procedura di Internal Audit*

	La procedura descrive come vengono eseguite le attività di audit.
Asset Management	*LEVA - Politica di Asset Management* Processo che descrive come le risorse vengono ricevute, etichettate, documentate ed eventualmente smaltite all'interno di LEVA.
Identity and Access Management	*LEVA - Politica Gestione degli Accessi e delle Identità* Descrive i requisiti generali per il controllo degli accessi e la creazione di ruoli e concetti di autorizzazione.
Supplier Management	*LEVA - Acquisti (NI 09.01 quality agreement - NI 09.02 condizioni generali di acquisto - NI 10.10 apqp - NI 10.30 acquisti)* Procedura che disciplina gli aspetti dei rapporti con i fornitori di prodotti e servizi.
IT Infrastructure Management Administrative special access	*LEVA - Politica Gestione Infrastruttura Tecnologica* Descrive i requisiti generali per i processi di gestione dell'infrastruttura IT, gestione della rete (incluse VPN e wi-fi), antivirus e antimalware, gestione delle modifiche, gestione delle patch e gestione della crittografia dei dati.
Log management	*LEVA - Politica di Log Management* Descrive i requisiti generali per la gestione dei log.
Backup Management	*LEVA - Politica di Backup e Ripristino* Processo che descrive la modalità di backup dei dati e dei sistemi.
Incident Management	*LEVA - Politica Gestione degli Incidenti* Descrivere le procedure messe in atto da LEVA al fine di garantire un approccio coerente ed efficace alla gestione degli incidenti di sicurezza delle informazioni.
Performance Measurement	*LEVA - Procedura di Misurazione dei KPI* Report contenente la definizione degli indicatori e delle misurazioni della performance.

6. Applicazione aziendale della politica di sicurezza delle informazioni

Le dichiarazioni di politica presentate in questo documento e nel set di politiche di supporto elencate nella tabella sopra sono state esaminate e approvate dalla dirigenza di vertice di LEVA e devono essere rispettate. Eventuali domande riguardanti qualsiasi politica di LEVA dovrebbero essere indirizzate in prima istanza al responsabile diretto dell'impiegato, o all'indirizzo e-mail **m.cirillo@levaspa.com per ambito IT itdepartment@levaspa.com.**

7. Revisione ed approvazione

La revisione e l'approvazione di questo documento sono di responsabilità della Direzione.

La Direzione di
LEVA S.p.a.