Politica Aziendale per la Sicurezza delle Informazioni

POL_PSI Rev. 08 del 15/04/2021

COLIBRÌ Video Insight S.r.l.
Via Adriano Olivetti, 24/26 - 00131 Roma RM
T [+39] 06 41204467 - F [+39] 06 41228120
colibrivideoinsight.com
Partita IVA 06464041000

CONTESTO E MOTIVAZIONE

Colibrì Video Insight S.r.l. è una società di ingegneria specializzata nella progettazione e sviluppo di sistemi ed applicazioni embedded ed in particolare di soluzioni ad alto contenuto tecnologico, che opera prevalentemente nei settori della Difesa, dell'Aerospazio e della Security.

Colibrì Video Insight ritiene che l'adozione di un sistema di Gestione per la Sicurezza delle Informazioni certificato rispetto alla norma UNI CEI ISO/IEC 27001:2017 abbia un valore strategico e rappresenti il framework nel cui valutare le misure tecniche e organizzative da adottare per assicurare l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo interno sia di quello dei propri Clienti. In particolare, per quanto riguarda le attività nel settore militare Colibrì Video Insight già si attiene alle relative normative in materia di sicurezza e intende fornire analoghe garanzie anche ai propri Clienti del settore civile tramite la certificazione UNI CEI ISO/IEC 27001:2017.

Le parti interessate pertinenti al Sistema di Gestione per la Sicurezza delle Informazioni, rispetto alle quali Colibrì Video Insight determina e recepisce i requisiti attinenti la sicurezza delle informazioni, sono rappresentate da: tutti i Clienti a cui sono rivolti i prodotti e servizi di Colibrì Video Insight, i partner con cui Colibrì Video Insight opera, la Direzione.

In quest'ottica, Colibrì Video Insight pone particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione, sviluppo, realizzazione e manutenzione dei propri prodotti, che devono essere ritenuti un bene primario dell'azienda. Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione del prodotto, ai servizi e ai dati ad esse collegate. In particolare alla tutela dei codici sorgenti, del loro corretto versionamento.

Consapevole del fatto che le proprie attività di progettazione e sviluppo per soggetti esterni possono comportare l'affidamento di dati e informazioni critiche, l'unità organizzativa tecnica opera secondo normative di sicurezza internazionalmente riconosciute.

OBIETTIVI

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di Colibrì Video Insight è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali, attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il Sistema di Gestione per la Sicurezza per le Informazioni di Colibrì Video Insight definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- Riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- Integrità, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre con la presente politica Colibrì Video Insight intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni :

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente
- Proteggere il proprio patrimonio informativo
- Evitare al meglio ritardi nella delivery

- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalizzazione
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza;

CONTENUTO DELLA POLITICA

Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione di prodotti integrati hardware/software o solo software, ai servizi e ai dati ad esse collegate, alla tutela del prodotti e ala relativa gestione della configurazione.

Tutte le informazioni, che vengono create o utilizzate dall'Azienda sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti. È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito della progettazione e sviluppo, tale sistema prevede – in conformità alla norma UNI CEI ISO/IEC 27001:2017 – che il Resp. per la Sicurezza delle Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi durante tale periodo e dei cambiamenti strategici, di business e tecnologici avvenuti; l'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate. La Direzione condivide con il Resp. della Sicurezza delle Informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella redazione della metodologia la Direzione partecipa anche alla definizione delle scale di valori da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio. In seguito dell'elaborazione dell'analisi dei rischi da parte del Resp. per la Sicurezza delle Informazioni in base alla metodologia condivisa con la Direzione, la Direzione stessa valuta i risultati ottenuti valutando e stabilendo di volta in volta la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere che saranno classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessaria di mantenere la conformità alle norme e leggi vigenti. Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

RESPONSABILITÀ:

- ***TUTTO IL PERSONALE*** che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.
- ***COMITATO DELLA SICUREZZA DELLE INFORMAZIONI:*** viene istituito un comitato della sicurezza che si incontrerà con cadenza almeno semestrale**.** È composto, in forma stabile, dall'Amministratore Unico e dal Responsabile della Sicurezza delle Informazioni. Vengono coinvolti a livello di comitato le competenze tecniche necessarie per la valutazione di aspetti specifici (es: Direttore Operations).

Ha il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza coerentemente alle politiche e alle linee strategiche aziendali definite.

RESPONSABILE DELLA SICUREZZA DELLE INFORMAZIONI Si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

- emanare tutte le norme necessarie ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di Colibrì Video Insight;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni;

- ***TUTTI I SOGGETTI ESTERNI*** che, intrattengono rapporti con Colibrì Video Insight devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

APPLICABILITÀ

La presente politica si applica indistintamente a tutti gli organi dell'Azienda. L'attuazione della presente politica è obbligatoria per tutto il personale Colibrì Video Insight e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda.

Colibrì Video Insight consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

RIESAME

Colibrì Video Insight verificherà periodicamente l'efficacia e l'efficienza del Sistema di Governo per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

Roma, 15 aprile 2021

L'Amministratore Unico

Dott. Carmine Caretta