POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Approvato dal CDA – Aprile 2019

EsseQuamVideri S.r.l.
00185 Roma, via S.Martino della Battaglia n° 31/B
CF, PI 06518181000 – R.E.A. n. 973349, CCIAA di Roma
Riferimento: rino.belloni@eqv.it - mob. 338 2292333

1. Premessa

EsseQuamVideri s.r.l. (qui di seguito definita "EsseQuamVideri" o "la Società") è una società di sviluppo software e consulenza IT. Data la natura delle proprie attività, la Società considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.

EsseQuamVideri pone particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione e sviluppo dei propri servizi e prodotti, che devono essere ritenuti un bene primario dell'azienda.

Il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione dei prodotti e servizi, ed ai dati ad esse collegati.

Consapevole del fatto che i propri servizi per soggetti esterni possono comportare l'affidamento di dati e informazioni sensibili, l'azienda si impegna ad operare secondo normative di sicurezza internazionalmente riconosciute.

Per questo motivo si intende adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'**integrità**, la **riservatezza** e la **disponibilità** sia del patrimonio informativo interno che di quello affidato dai propri Clienti.

Su tali basi EsseQuamVideri ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) definito secondo regole e criteri previsti dagli standard internazionali di riferimento in conformità alle indicazioni della norma internazionale ISO/IEC 27001:2014.

2. Normative in materia

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- D.lgs. 231/2001, art.24-bis "Delitti informatici e trattamento illecito di dati";
- D.lgs. 169/99 "Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di

- dati";
- D.lgs. 259/2003 "Codice delle comunicazioni elettroniche";
- D.lgs. 196/2003 "Codice in materia di protezione dei dati personali";
- Provvedimento del Garante per la Protezione dei Dati Personali "Misure di sicurezza obbligatorie per le intercettazioni" (Provvedimento del 15 settembre 2005);
- Provvedimento del Garante per la Protezione dei Dati Personali "Misure e disposizioni volte a salvaguardare gli interessati in relazione alla conservazione dei dati relativi al traffico telefonico e Internet per l'individuazione e la soppressione dei reati" (Provvedimento del 17 gennaio 2008);
- Provvedimento del Garante per la Protezione dei Dati Personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di Sistema" (Provvedimento del 27 novembre 2008);
- Legge 22 aprile 1941, n.633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";
- Provvedimento del Garante per la Protezione dei Dati "Misure concernenti la videosorveglianza" (Provvedimento del 8 aprile 2010);
- Legge 23 dicembre 547/93 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";
- Legge 18 marzo 48/2008 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" (Convenzione di Budapest).

Standard di riferimento

- ISO/IEC 27001:2013 "Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti";
- ISO/IEC 27000 "Tecnologie informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza dell'informazione – Descrizione e vocabolario".

2. Obiettivi

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

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

• **RISERVATEZZA**: l'informazione deve essere nota solo a chi dispone di opportuni privilegi;

• **INTEGRITÀ**: l'informazione deve essere modificabile solo ed esclusivamente da chi ne possiede i privilegi;

• **DISPONIBILITÀ**: l'informazione deve essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che dispongono dei relativi privilegi.

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

• Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;

• Proteggere al meglio il patrimonio informativo proprio e dei propri clienti;

• Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità;

• 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 sia hardware che software, ai servizi e ai dati ad esse collegati, alla tutela dei prodotti e alla 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 ISO/IEC 27001:2014 – che il Responsabile 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 Responsabile 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 valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.

In seguito dell'elaborazione dell'analisi dei rischi da parte del Responsabile per la Sicurezza delle Informazioni ed in base alla metodologia condivisa con la Direzione, la Direzione stessa valuta i risultati ottenuti accogliendo 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 necessità di mantenere la conformità alle norme eleggi vigenti.

3. Distribuzione ed applicabilità

La presente politica è distribuita mediante il sito internet aziendale, che ne mette a disposizione la versione approvata più aggiornata. Qualunque copia di questo documento non sia appena stata scaricata dal sito internet aziendale è da considerarsi non aggiornata. Di conseguenza, è responsabilità del lettore assicurarsi di ottenere la versione più aggiornata ed attuale del documento.

La presente politica si applica indistintamente a tutti gli organi dell'Azienda. L'attuazione della presente politica è obbligatoria per tutto il personale 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.

La Società 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.

4. Riesame

Così come stabilito dalla ISO 27001, EsseQuamVideri verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione 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.

Il presente documento integra e non sostituisce il documento denominato "Procedura per la Gestione dei Dati e Misure di Sicurezza" (SGI-PGDS-001).