

Politica per la Sicurezza delle Informazioni

Hyris opera nel campo delle biotecnologie, in particolare nel campo dell'analisi genetica delocalizzata. La tecnologia che abbiamo sviluppato comprende hardware, software e reagenti, che insieme permettono di verificare la presenza o meno di materiale genetico bersaglio in un campione incognito. La tecnologia trova applicazioni sia in campo industriale (controllo qualità, sicurezza alimentare...) che in campo medico (e.g. diagnostica). La mission della nostra azienda è sia rendere l'analisi genetica progressivamente alla portata di tutti, abbassando il costo e la complessità richieste, sia creare un vero e proprio network di analisi, con migliaia di macchine distribuite nel mondo e connesse da un servizio software cloud.

Portare, nel campo dell'analisi genetica distribuita, l'innovazione dirompente del *Software as a Service* richiede all'azienda di mettere, tra i suoi obiettivi primari, la protezione della sicurezza delle informazioni che le vengono affidate dai clienti.

In ragione di ciò Hyris ha deciso di strutturare ed orchestrare la propensione alla sicurezza innata nell'azienda attraverso la costruzione di un sistema di gestione unificato che risponda ai seguenti requisiti:

- **Protezione:** il sistema di gestione deve assicurare la protezione delle informazioni dei clienti e della compagnia
- **Conformità:** il sistema di gestione deve essere conforme ai requisiti di legge nazionali ed internazionali, in particolare le leggi di protezione della privacy (General Data Protection Regulation 2016/679), del lavoro (Testo unico per la sicurezza sul lavoro Dlgs 81/2008)
- **Dimostrabilità:** il sistema di gestione deve essere dimostrabile nella sua efficacia attraverso l'adesione a standard riconosciuti internazionalmente, nello specifico lo standard **ISO/IEC 27001**
- **Generalità:** il sistema di gestione deve essere il più possibile generalizzato così da adattarsi ai cambiamenti tecnologici e di processo interni all'azienda
- **Migliorabilità:** il sistema di gestione deve riesaminare periodicamente i propri obiettivi e la propria efficacia intraprendendo un processo di miglioramento continuo con una periodicità non superiore ad i 12 mesi
- **Integrazione:** il sistema di gestione deve soprassedere ed integrarsi ai processi aziendali esistenti

Stabiliti i requisiti del sistema di gestione della sicurezza la direzione si impegna ad affidarne la realizzazione a personale competente supportandone il lavoro attraverso:

- L'accesso a corsi di formazione specifici
- Lo stanziamento di un budget adeguato

Il presente documento costituisce un impegno, da parte della compagnia, nella costruzione di un approccio strutturato e ripetibile alla sicurezza delle informazioni che viene riconosciuta come valore fondamentale della compagnia all'interno del mercato di riferimento.

I documenti costitutivi l'information security management system sono disponibili sul sito internet dell'azienda e condivisi su richiesta con le parti interessate nel rispetto della normativa interna, delle norme contrattuali e delle leggi vigenti.

Tutti i documenti costitutivi l'information security management system vengono rivisti con cadenza almeno annuale e valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio
- significativi incidenti di sicurezza
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle