OFFERTA TECNICA

1. Servizio di consulenza

La presente offerta tecnica è stata elaborata in risposta alla procedura di affidamento del servizio di consulenza per la corretta ed efficace conduzione e il continuo miglioramento del Sistema di Gestione Integrato (SGI) di FONDIMPRESA, con specifico focus sugli adempimenti inerenti alla norma ISO 9001, ISO/IEC 27001 in materia di sicurezza delle informazioni e include anche la gestione dei processi a garanzia della protezione dei dati personali ai sensi del Reg. (UE) 2016/679 (GDPR) e del Codice Privacy.

Il servizio di consulenza ha lo scopo di supportare FONDIMPRESA nel mantenimento e nell'aggiornamento del proprio SGI, garantendo il rispetto dei requisiti normativi e delle best practice internazionali in materia di sicurezza delle informazioni.

Inoltre, la presente offerta tecnica descrive in dettaglio le caratteristiche, le funzionalità e i benefici della soluzione software SaaS "KEYMAP" per la gestione delle norme ISO 9001, ISO/IEC 27001 e GDPR, nonché le modalità di erogazione del servizio di consulenza e le competenze del nostro team di esperti.

Abbiamo utilizzato le specifiche del bando di gara per delineare le modalità operative proposte per la gestione dei servizi richiesti. Di seguito il dettaglio per ciascun requisito del bando di gara.

2. Attività oggetto dell'affidamento

Di seguito le attività oggetto dell'affidamento con il dettaglio delle inclusioni:

1. **La procedura di affidamento ha per oggetto il servizio di consulenza per la corretta ed efficace conduzione e il continuo miglioramento del SGI, con specifico focus sugli adempimenti inerenti alla ISO/IEC 27001 in materia di sicurezza delle informazioni.**

FONDIMPRESA è un organismo complesso chiamato a rispondere del proprio operato sotto diversi profili di conformità. Nel tempo ha implementato e sta implementando un numero crescente di sistemi di gestione conformi a standard volontari e modelli normativi per rispondere agli adempimenti imposti dalla legislazione cogente; fra questi quelli individuati nel bando di gara sono la norma ISO 9001 per il sistema di gestione per la qualità, ISO/IEC 27001 in materia di sicurezza delle informazioni e GDPR.

Per governare tale scenario, l'organizzazione ha la necessità di tenere costantemente aggiornati i propri sistemi e modelli normativi al fine di garantire il rispetto del principio della cosiddetta "dynamic compliance": cambiamenti organizzativi, normativi, procedurali, e di risorse/asset modificano la valutazione dei rischi a cui sono esposte le informazioni e i dati personali e devono essere pertanto costantemente monitorati e gestiti al fine di poter procedere all'identificazione delle contromisure adeguate a garantire la sicurezza delle informazioni dell'organizzazione.

2. **Le attività oggetto dell'affidamento devono includere, tra l'altro: l'individuazione degli adempimenti previsti dalle norme ISO 9001 e ISO/IEC 27001, in rapporto allo stato del Sistema di Gestione del Fondo;**

Per fare questo l'organizzazione ha bisogno di verificare in primis che tutti gi adempimenti previsti dai sistemi ISO 9001, ISO/IEC 27001 e GDPR siano rispettati e correttamente implementati nel rispetto del proprio contesto di riferimento (ossia allo stato di gestione del Fondo).

Questa analisi verrà svolta tramite un'attività di Gap Analysis basata sulla documentazione esistente e, ove necessario, tramite interviste mirate con le risorse coinvolte. Gli obiettivi di questa fase sono:

- garantire che tutti i requisiti siano stati soddisfatti,
- trovare eventuali aree di debolezza e carenze da affrontare,
- dare una priorità alle azioni correttive da attuare.

3. **La conduzione degli audit interni, con copertura annuale di tutti i processi, comprensiva della redazione dei verbali e degli eventuali follow up necessari;**

Le attività di audit verranno svolte in base al seguente iter procedurale:

- predisposizione di un piano di Audit che includa tutti i processi mappati nel Sistema di Gestione Integrato ISO 9001 e ISO/IEC 27001;
- identificazione, per ciascun processo, dei process owner e degli eventuali referenti/responsabili da coinvolgere nell'attività di audit (eventualmente anche soggetti esterni all'organizzazione);
- costituzione di un team di auditor multidisciplinare in grado di garantire adeguata copertura tecnica e metodologica rispetto alle tematiche da sottoporre a verifica;
- esecuzione degli audit nelle date nei luoghi e con le modalità definite nel piano;
- predisposizione di Report di Audit e condivisione delle risultanze con Referenti;
- definizione di un Action Plan con le azioni concordate per la chiusura di eventuali gap riscontrati come osservazioni, non conformità o opportunità di miglioramento;
- monitoraggio e verifica della presa in carico ed implementazione delle azioni correttive in base alle responsabilità e alle scadenze previste.

4. **Il supporto per il mantenimento e l'aggiornamento continuo della mappatura delle informazioni ai sensi della ISO/IEC 27001;**

Aggiornamento e controllo periodico, per ciascun processo dell'organizzazione, delle categorie di informazioni trattate, compresi i dati personali e loro classificazione in termini di riservatezza, integrità e disponibilità (informazioni riservate, ad uso interno, pubbliche…) e valutazione del relativo impatto.

AREA	MACROPROCESSO	PROCESSO	TIPO DATO	OWNER DATI
AFC	Gestione tesoreria e credito		Dati bancari	TRCR
AFC	Gestione tesoreria e credito		Dati contrattuali bancari	TRCR
AFC	Gestione tesoreria e credito		Dati pagamento clienti	TRCR
AFC	Gestione tesoreria e credito		Dati pagamento clienti	TRCR
CCO	Gestione comunicazione in caso di crisi		Dati modalità di gestione processi	CCO
CCO	Gestione social media e online communication		Dati amministrativo-contabili di società	CAO
CCO	Gestione social media e online communication		Dati comunicazioni ufficiali	CCO
CCO	Gestione social media e online communication		Dati economico-finanziari	CAO
CCO	Gestione social media e online communication		Dati economico-finanziari di società	CCO
CCO	Gestione social media e online communication		Dati immagine e multimediali di prodotto	CCO
CCO	Gestione social media e online communication		Dati news interne	CCO
CCO	Gestione social media e online communication		Dati omaggi e ospitalità	CCO
CCO	Gestione social media e online communication		Dati utilizzo portale	CCO
DIV-COMM	Gestione commerciale		Dati capacità produttive clienti	SALES
DIV-COMM	Gestione commerciale		Dati contabilità gestionale	CFCO
DIV-COMM	Gestione commerciale		Dati contabilità gestionale	CFCO
DIV-COMM	Gestione commerciale		Dati contrattuali	SALES
DIV-COMM	Gestione commerciale		Dati contrattuali	SALES
HRO	Gestione risorse umane	Gestione amministrativa del rapporto di lavoro	Dati anagrafici del personale	CHRO

5. **Il supporto alla stesura della documentazione del SGI;**

Verrà dato il supporto necessario alla gestione della documentazione dell'SGI tramite:

- stesura, revisione e aggiornamento di Manuale, Politiche e Procedure;
- predisposizione/aggiornamento dell'elenco di documenti, dei moduli e delle registrazioni;
- stesura dei rapporti di Audit e dell'Action Plan;
- supporto all'aggiornamento del Riesame della Direzione.

6. **L'affiancamento nel corso delle visite dell'ente terzo di certificazione per gli audit di mantenimento e per gli audit di ricertificazione e la presa in carico dei conseguenti rilievi;**

È prevista un'attività di supporto sia in termini documentali che operativi ai responsabili interni durante la vista dell'Ente di Certificazione. L'obiettivo è mettere a disposizione di FONDIMPRESA un team di consulenti con adeguate competenze sia tecniche che organizzative in modo da fornire il miglior sostegno possibile durante la verifica.

A valle dell'audit di terza parte verranno condotte le seguenti attività:

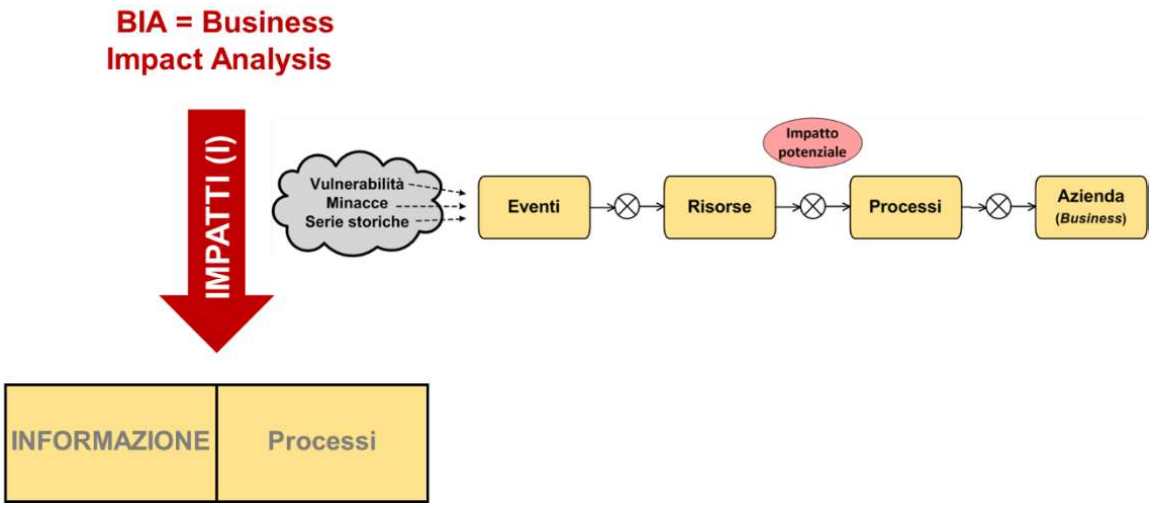
- identificazione delle azioni correttive necessarie;
- implementazione delle azioni correttive definite.

7. L'analisi dei processi di sicurezza delle informazioni esistenti e dei presidi adottati;

Verranno condotte Interviste con gli owner di processo e verrà eseguita un'analisi della documentazione esistente in relazione alle modalità operative di gestione dei processi di sicurezza delle informazioni e ai presidi adottati (situazione as is). Valutazione dell'efficacia e dell'efficienza dei processi di sicurezza in uso.

8. L'esecuzione della Business Impact Analysis (BIA);

- Valutazione delle conseguenze di una violazione di riservatezza, integrità e disponibilità dei dati, compresi quelli personali, per ciascun processo individuato;
- Definizione della soglia di propensione al rischio e di quelle di impatto minimo (soglia di indifferenza) e massima (soglia di cessazione);
- Individuazione delle minacce cui il patrimonio informativo è sottoposto;
- Stima del grado di protezione offerto dai controlli attualmente in essere;
- Esecuzione della BIA (Business Impact Analysis).

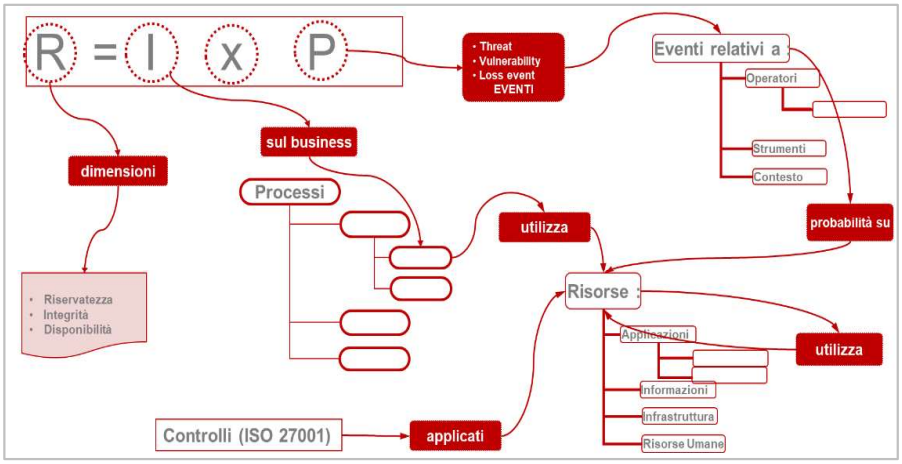


Servizio Commerciale	Analisi impatto (BIA)												
	Riservatezza			*Integrità*			*Disponibilità*			*Conformità*			*Privacy*
	Economico	*Normativo*	*Reputazionale*	*Economico*	*Normativo*	*Reputazionale*	*Economico*	*Normativo*	*Reputazionale*	*Economico*	*Normativo*	*Reputazionale*	*Impatto violazione dati personali*
Servizio formazione tutoring	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1- Trascurabile**
Consulenza GDPR - Supporto gestione adempimenti	**1**	**4**	**4**	**1**	**3**	**3**	**1**	**1**	**1**	**2**	**3**	**3**	**1- Trascurabile**
Prodotto IT per gestione documentale e protocollo	**2**	**2**	**2**	**3**	**3**	**3**	**2**	**3**	**3**	**2**	**3**	**3**	**3 - Significativo**

9. Le valutazioni dei rischi ai sensi della ISO 9001 e della ISO/IEC 27001, inclusi l'analisi critica e l'eventuale aggiornamento delle metodologie del Fondo;

In ottica ISO/IEC 27001 verrà condotto un risk assessment attraverso i seguenti passaggi:

- identificare le risorse che contengono o gestiscono informazioni che necessitano di protezione;
- determinare le potenziali minacce a ogni asset e le vulnerabilità che potrebbero essere sfruttate da tali minacce;
- valutare l'impatto che ciascun rischio potrebbe avere sull'organizzazione e la probabilità che il rischio si verifichi;
- calcolare il livello di rischio combinando l'impatto e la probabilità;
- decidere come affrontare ciascun rischio identificato.

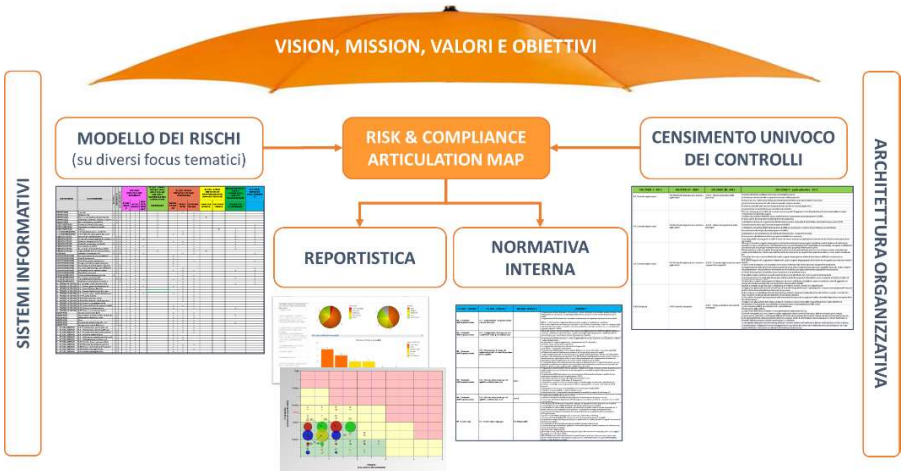


Dal punto di vista ISO 9001 l'analisi dei rischi verrà condotta attraverso le seguenti modalità:

- Identificare gli scenari di rischio (eventi) che possono interessare i diversi processi dell'organizzazione;
- Pesatura dei rischi in base ai livelli di probabilità ed impatto definiti coi responsabili di processo;
- Mappatura delle azioni correttive già implementate dall'organizzazione e definizione del livello di rischio as is;
- Individuazione delle opportune azioni di mitigazioni che hanno impatto su probabilità e /o impatto degli eventi di rischio;
- Stima del grado di rischio residuo a valle dell'implementazione delle contro misure.

Verrà svolta un'analisi critica delle metodologie di calcolo del rischio utilizzata dal fondo al fine di valutare un adeguamento delle prassi operative volto ad una:

- definizione di una metodologia univoca per la gestione dei rischi per ciascun ambito (focus normativo) al fine di ottenere analisi comparabili e compatibili;
- costruzione di un unico database dei rischi integrato e di un censimento univoco dei controlli in modo da sfruttare sinergie e trasversalità rispetto ai differenti focus tematici;
- predisposizione di un unico pannello di controllo, tramite la piattaforma KEYMAP, per gli indicatori di performance collegati ai rischi, agli obiettivi strategici e ai processi dell'organizzazione.



10. La valutazione del livello di maturity delle misure tecniche e organizzative applicate da Fondimpresa per la sicurezza delle informazioni;

Occorre verificare per ciascun evento le misure organizzative e i presidi eventualmente già posti in essere nell'organizzazione, al fine di valutare eventuali scostamenti. La Gap Analysis tra il modello esistente «AS IS» e il modello a tendere «TO BE» mette in evidenza le azioni correttive necessarie per l'implementazione di nuovi standard di controllo o il miglioramento di quelli esistenti. L'obiettivo è quello di riportare / mantenere il rischio (c.d. "residuo") ad un livello accettabile per l'organizzazione. La metodologia utilizzata per valutare il livello di maturity delle contromisure prevede l'utilizzo del seguente scala:

VALORE	TITOLO	CRITERIO
0	**PROCESSO INCOMPLETO**	il processo non viene implementato o non riesce a raggiungere il suo scopo. A questo livello esiste scarsa o nessuna evidenza di raggiungimento sistematico della finalità di processo.
1	**PROCESSO ESEGUITO**	il processo implementato raggiunge il suo scopo.
2	**PROCESSO GESTITO**	il processo eseguito viene ora implementato secondo una determinata gestione (pianificazione, monitoraggio e adattamento) e i suoi prodotti di lavoro vengono opportunamente stabiliti, controllati e mantenuti.
3	**PROCESSO DEFINITO**	il processo gestito, descritto in precedenza, viene ora implementato utilizzando un processo definito in grado di conseguire i propri risultati.
4	**PROCESSO PREVEDIBILE**	il processo definito, precedentemente descritto, ora funziona entro limiti definiti per raggiungere i suoi risultati.
5	**PROCESSO IN OTTIMIZZAZIONE**	il processo prevedibile, precedentemente descritto, viene continuamente migliorato per soddisfare importanti obiettivi aziendali, attuali e previsti.

11. L'individuazione di presidi/processi di sicurezza delle informazioni adeguati secondo quanto previsto dalle best practice internazionali in materia (norme della famiglia ISO/IEC 27000, ENISA Framework, NIST Cybersecurity Framework, etc.);

In funzione delle risultanze dell'analisi di cui al punto precedente, effettuazione delle valutazioni costo-beneficio e individuazione dei presidi di sicurezza necessari a contenere i rischi individuati sulla base dei controlli proposti dalle linee guida di riferimento da Voi indicate.

12. Il supporto per la progettazione, definizione e attuazione di presidi e processi di sicurezza.

Per ciascun presidio di controllo, sarà eseguito un disegno e una formalizzazione di processi e dei piani di sicurezza/continuità utilizzando modalità operative in conformità alle best practice internazionali in tema di sicurezza informatica (norme della famiglia ISO/IEC 27000 sulla sicurezza delle informazioni, NIST Cybersecurity Framework, ENISA Framework).

Progettazione dei controlli, sia documentali che operativi: raccolta informazioni per la documentazione, pianificazione di dettaglio dei controlli operativi.

Attuazione dei controlli progettati, in affiancamento ai responsabili di processo e di attività.

VARIAZIONE CONTRATTUALE

Qualora Fondimpresa decidesse di variare in aumento il contratto nel corso della sua esecuzione, ai sensi dell'art. 120, comma 1, lett. a) del Codice dei contratti pubblici, GRCteam è pronta a integrare il contratto per le attività di caricamento delle informazioni relative alle norme ISO 9001, ISO/IEC 27001 e GDPR nella piattaforma KEYMAP o alla esecuzione delle seguenti ulteriori attività.

13. Conduzione di attività formative su temi inerenti all'oggetto dell'appalto per i dipendenti del Fondo e/o delle Articolazioni Territoriali dello stesso.

Contestualmente alle fasi precedenti e attraverso la programmazione di sessioni dedicate, potranno essere effettuate attività di formazione e sensibilizzazione del personale in merito alle tematiche di sicurezza delle informazioni, inclusa l'integrazione ISO/IEC 27701 attraverso la predisposizione del materiale didattico e l'erogazione sessioni formative da concordare.

14. Supporto per la transizione a nuove edizioni delle norme ISO 9001 e/o ISO/IEC 27001.

Supporto per l'adeguamento dei sistemi di gestione di FONDIMPRESA ad eventuali nuove edizioni delle norme che dovessero nel frattempo essere pubblicate con l'implementazione dei nuovi requisiti al fine di garantire la continua conformità.

15. Estensione ISO/IEC 27701

Questa attività di consulenza consiste nella costruzione di un Sistema di Gestione della Riservatezza delle Informazioni (Privacy Information Management System, PIMS).
In merito ai requisiti in materia di protezione dei dati personali si prevede di integrare le fasi di cui sopra con le seguenti attività:

- analisi e revisione critica della mappatura delle attività di trattamento dati personali e delle informazioni correlate;
- analisi e revisione/valutazione dei rischi con particolare attenzione alle contromisure adottate per garantire la protezione dei dati personali. Contestuale verifica dell'eventuale necessità di conduzione di una DPIA;
- confronto tra le contromisure presenti nella gestione del rischio condotta secondo la metodologia ENISA e le contromisure indicate dalla norma ISO/IEC 27701;

- revisione, integrazione e aggiornamento documentazione, policy e procedure in funzione delle previsioni della ISO/IEC 27701;
- verifica e raccordo tra il sistema ISO/IEC 27701 e il GDPR.

16. Supporto alla conduzione di attività di audit sui fornitori o sulle Articolazioni Territoriali del Fondo.

Supporto per la conduzione di attività di audit di seconda parte sui fornitori o sulle articolazioni territoriali del fondo in base a modalità e numerosità da definire col cliente.

3. Soluzione Software SaaS – gestione integrata

Dotazione di soluzioni software in modalità SaaS (Software as a Service), per la gestione integrata delle norme

La soluzione proposta tiene conto dei requisiti elencati nel bando di gara e sotto è presente una prima risposta sintetica, a seguire una presentazione dettagliata delle principali funzionalità della piattaforma KEYMAP.

- **Mappatura di Processi, Responsabilità e Asset:** La piattaforma consente di mappare e gestire processi aziendali, responsabilità e asset in modo integrato.
- **Mappatura del Patrimonio Informativo:** Conforme alla norma ISO/IEC 27001, KEYMAP permette una gestione completa del patrimonio informativo del Fondo.
- **Registro dei Trattamenti ex art. 30 del GDPR:** La piattaforma include la gestione del registro dei trattamenti in conformità con l'articolo 30 del GDPR.
- **Attività di Audit:** Gestione integrata delle attività di audit, comprese registrazioni, verbali, controdeduzioni, notifiche e notifiche automatiche.
- **Rilievi:** Classificazione e gestione dei rilievi derivanti da audit e altre fonti, con tracciamento di stato, categoria, norma di riferimento, origine, responsabile, area/processo, oggetto, descrizione, analisi delle cause, trattamento, azione di miglioramento/correttiva.
- **Scadenzario dei Rilievi:** Gestione dello scadenzario per monitorare le scadenze relative ai rilievi.
- **Valutazione del Rischio:** Funzionalità per la valutazione continua del rischio associato alla conformità normativa.
- **Reportistica:** Generazione di report personalizzati e dettagliati per monitorare e presentare lo stato della conformità.

Caratteristiche Tecniche della Soluzione

- **Separazione dei Dati:** La piattaforma garantisce la separazione logica o fisica dei dati di Fondimpresa da quelli di altri clienti, assicurandone la protezione e la riservatezza.
- **Design Responsive:** L'interfaccia utente è adattabile a schermi di diverse dimensioni, inclusi tablet e smartphone.
- **Accesso Sicuro:** Fruibile tramite i più comuni browser (Chrome, Safari, Firefox, Edge) con accesso sicuro.
- **Best Practice di Secure Coding:** Sviluppata in accordo con le best practice di secure coding (ISO/IEC 27001, OWASP, NIST).
- **Storicizzazione delle Modifiche:** Include la storicizzazione delle modifiche effettuate nel tempo alla mappatura delle informazioni e al registro dei trattamenti.
- **Export dei Contenuti:** Consente l'export dei principali contenuti ospitati in formato PDF e/o Excel.

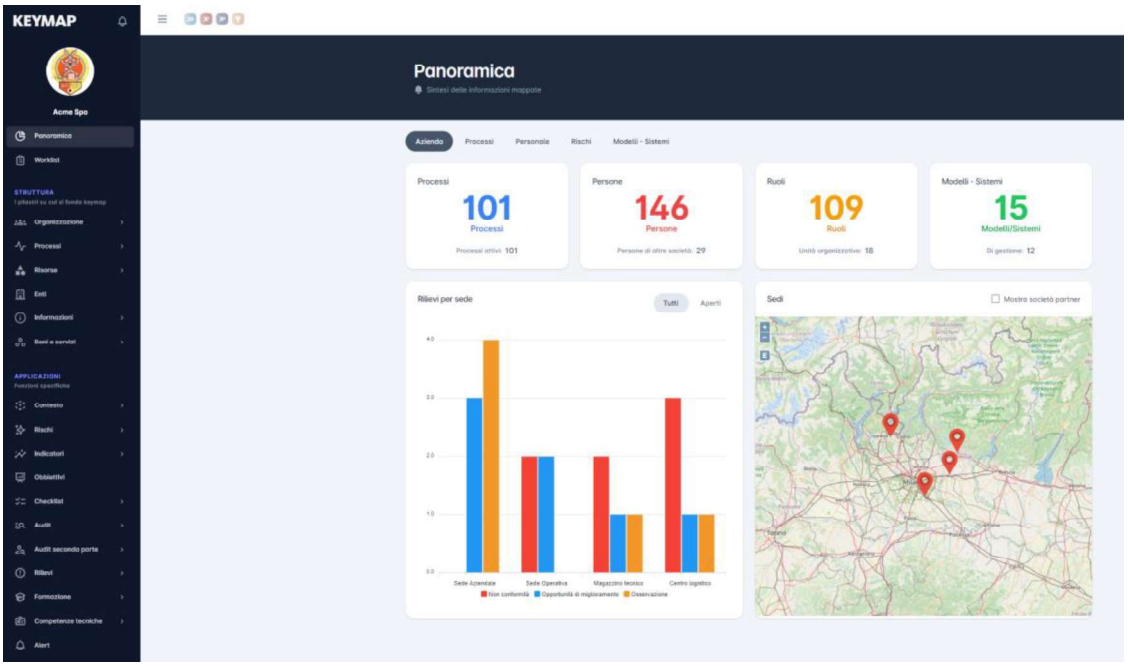
- **Esportazione Dati e Supporto alla Migrazione:** Supporto completo per l'esportazione di tutti i dati in un formato interoperabile e assistenza nella migrazione verso un nuovo applicativo alla scadenza dell'affidamento.

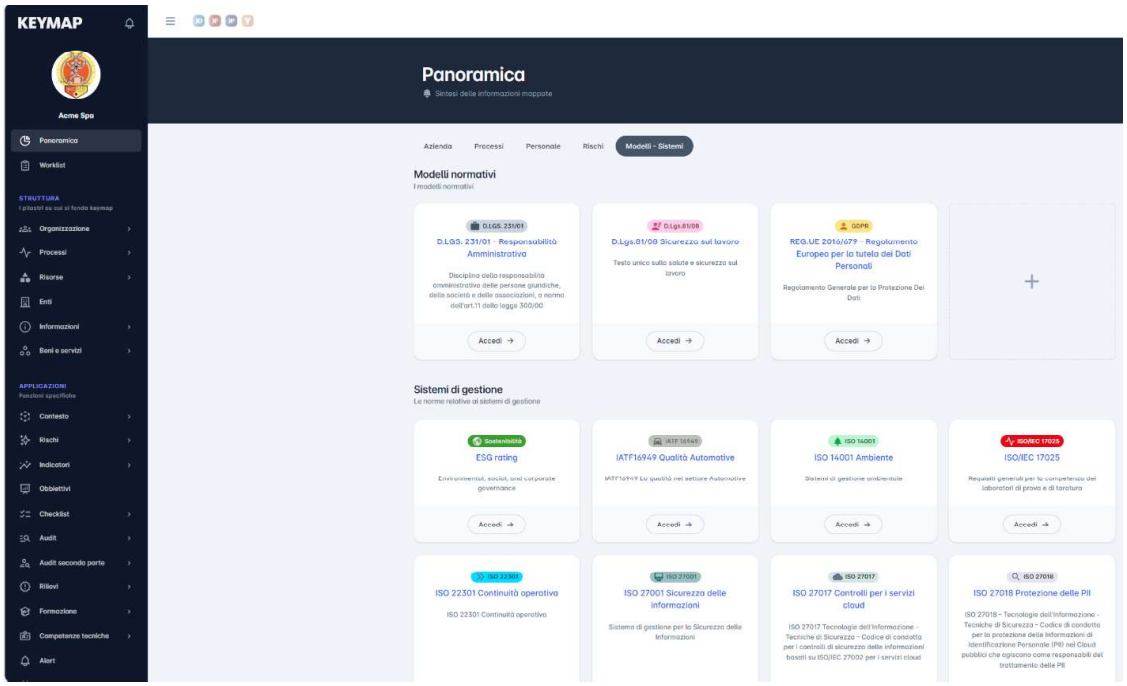
Di seguito una presentazione della soluzione software "KEYMAP" in modalità SaaS (Software as a Service). La piattaforma KEYMAP è progettata per garantire la gestione integrata di norme cogenti e sistemi di gestione, e offre un controllo completo su tutti gli elementi, le informazioni e i documenti necessari per assicurare la conformità normativa.

La piattaforma KEYMAP è registrata nel catalogo delle infrastrutture digitali e dei servizi Cloud dell'Agenzia per la cybersicurezza nazionale (ACN) e disponibile al seguente indirizzo:

- Keymap https://www.acn.gov.it/portale/w/sa-3000

Di seguito alcune immagini della piattaforma KEYMAP:





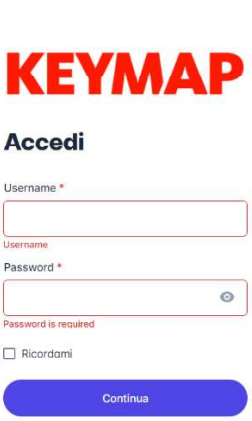
Seguono le funzionalità presenti nella piattaforma KEYMAP e dove utile una immagine esplicativa del prodotto.

Principali Funzionalità della Piattaforma KEYMAP:

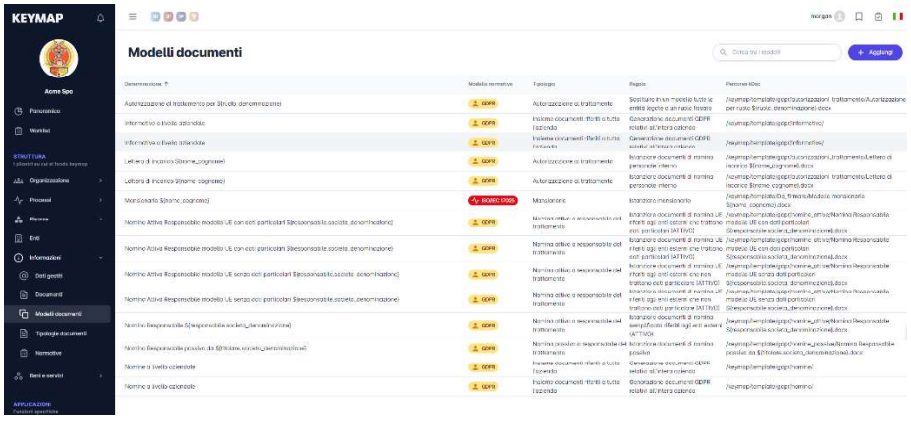
1. **Web Based**: la piattaforma è fruibile dal browser senza installazione di prodotti software sulla stazione di lavoro dell'utente, è design responsive per il suo uso anche tramite tablet e smartphone.
2. **Autorizzazioni utente**: la profilazione degli utenti consente di attivare funzionalità in base ai livelli autorizzativi concessi dall'azienda;
3. **Storicizzazione:** la piattaforma permette il mantenimento dei dati storici e la gestione delle revisioni dei modelli/sistemi e dei documenti.
4. **Interfacciabilità:** è possibile sviluppare collegamenti ad altri sistemi come piattaforme ERP, CRM, SSO ecc.
5. **Multiazienda:** gestisce più aziende facenti parte di un'unica holding, inclusa la gestione di aziende collegate in diverse località geografiche.
6. **Multilingua:** per ogni utente è possibile l'uso della lingua di riferimento tra quelle consentite dall'organizzazione.

Elementi Infrastrutturali che costituiscono la piattaforma KEYMAP:

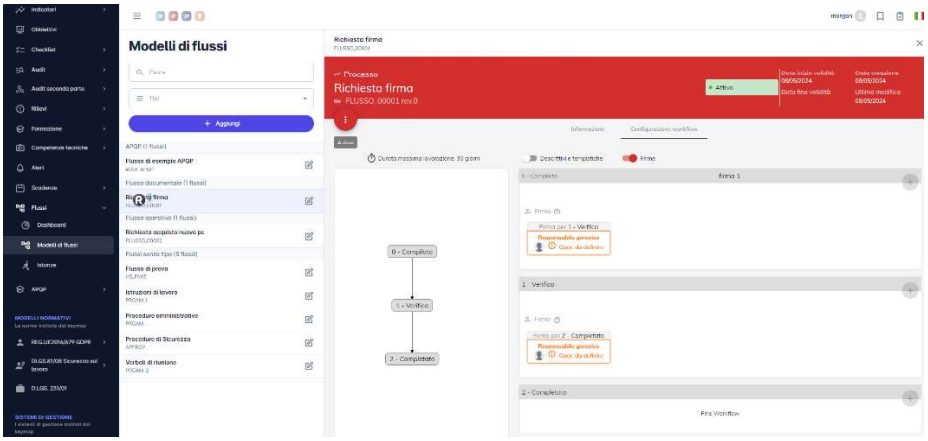
- Sistema di Autenticazione e Profilazione degli Utenti (**IMSIGN**);



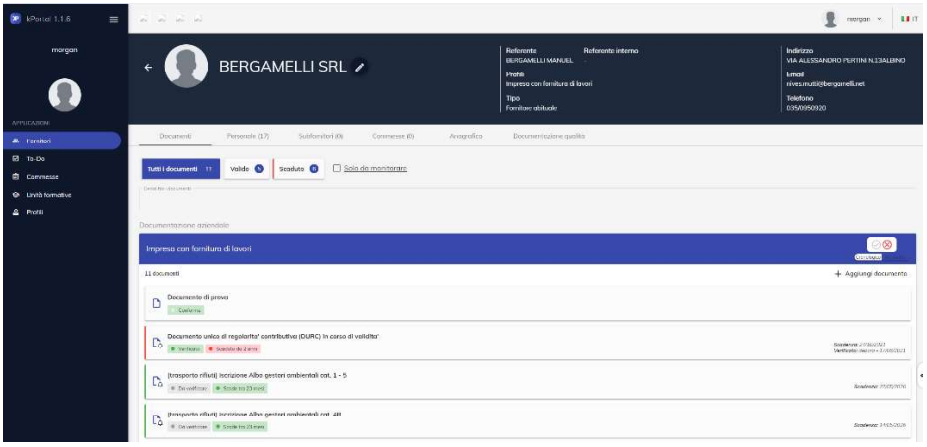
- Gestione Documentale (**KDOC**);



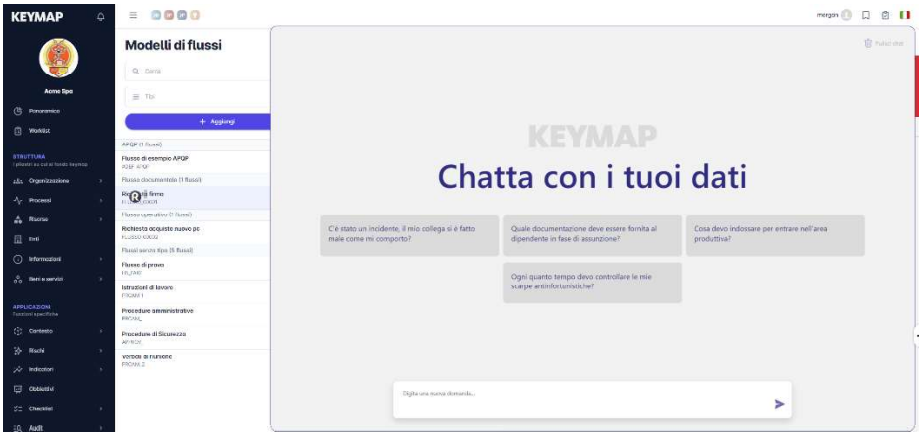
- Gestione dei Flussi Operativi (**KFLOW**);



- Relazione con i Fornitori (**KPORTAL**);



- Modulo di Intelligenza Generativa (**KAI**) (opzionale e non incluso nella presente offerta).



Funzionalità di Primo Livello

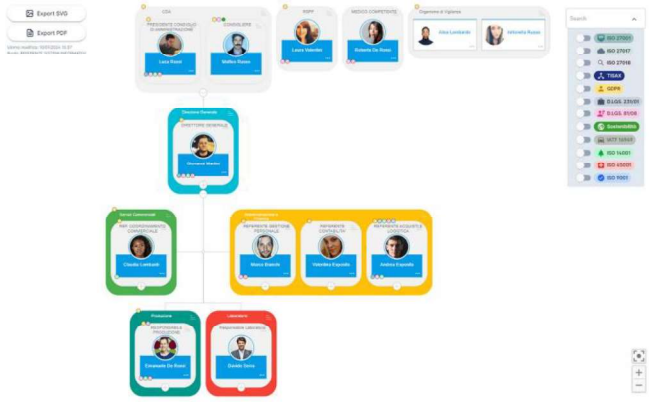
<u>Piattaforma KEYMAP: Struttura</u>

- **Organizzazione, unità organizzative, ruoli, persone**: Gestione dettagliata della struttura organizzativa, comprese le diverse unità, ruoli e personale.
- **Processi**: Definizione e gestione dei processi dell'organizzazione.
- **Risorse/assets**: Mappatura e gestione delle risorse dell'organizzazione.
- **Enti (partner, fornitori, etc.)**: Gestione delle relazioni con partner e fornitori.
- **Informazioni (dati, documenti, modelli)**: Gestione centralizzata delle informazioni, inclusi dati, documenti e modelli.

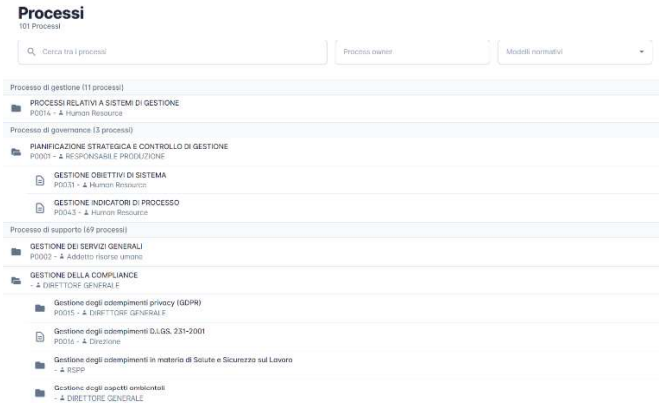
- **Beni e servizi**: Gestione di beni e servizi dell'organizzazione.

Seguono alcune immagini relative alla parte STRUTTURA di KEYMAP:

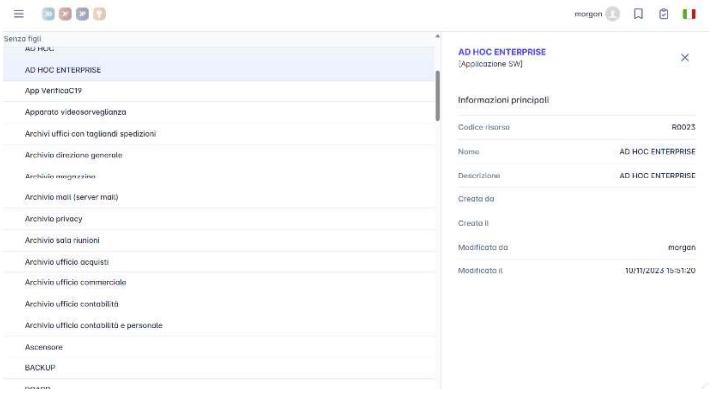
- **Organizzazione:** Unità organizzative, ruoli, persone e aziende collegate;



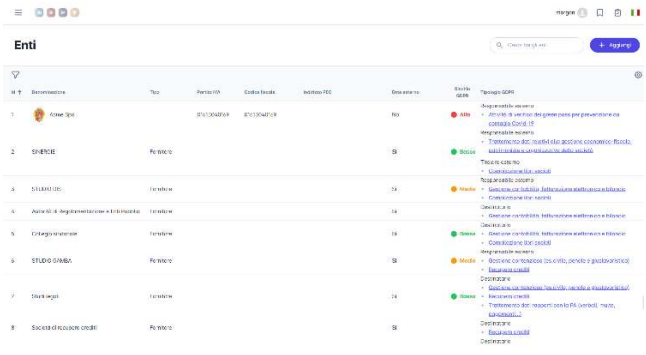
- **Processi:** gestione dei processi aziendali



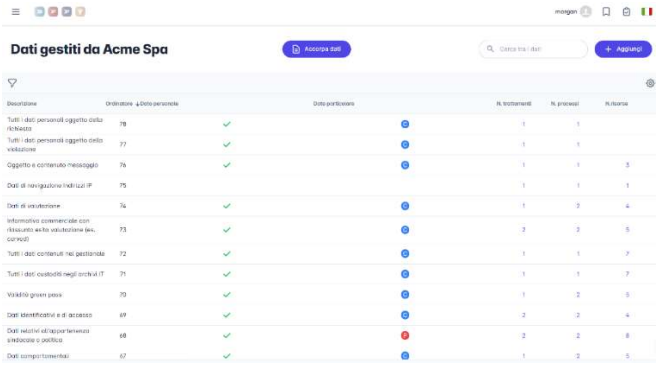
- **Risorse/Assets:** gestione dei diversi asset (impianti, hardware, software, locali tecnologici…)



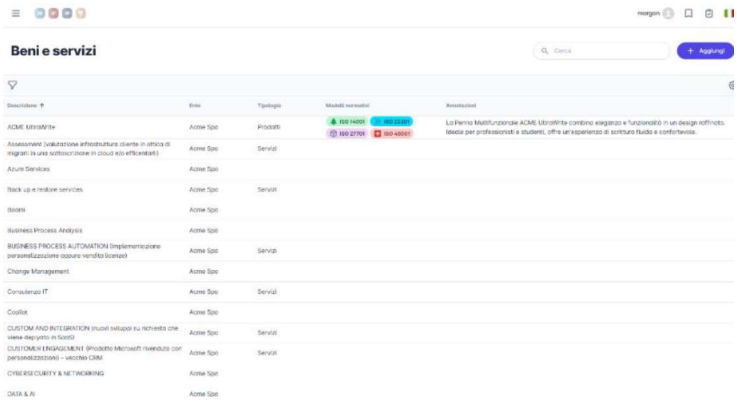
- **Enti:** Partner, fornitori, etc.



- **Informazioni:** Dati, documenti, modelli, norme.



- **Beni e Servizi:**

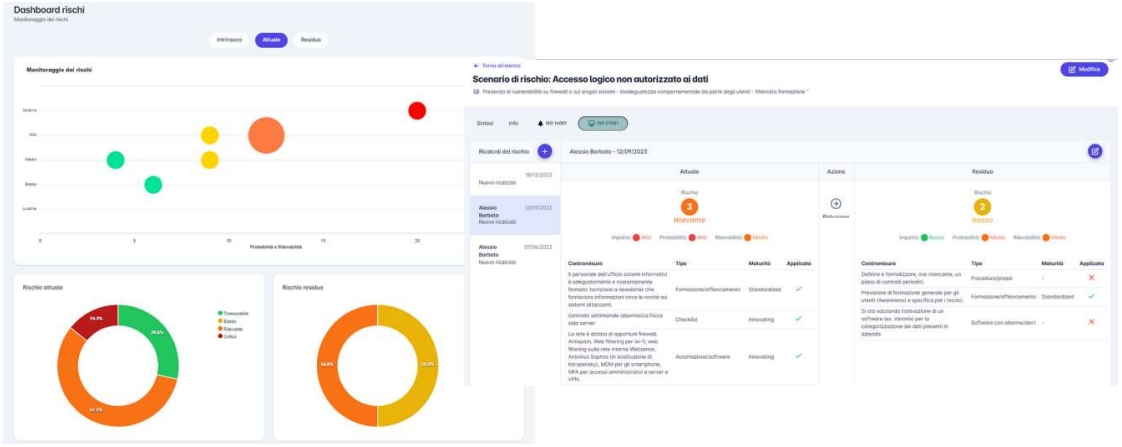


Piattaforma KEYMAP: Applicazioni

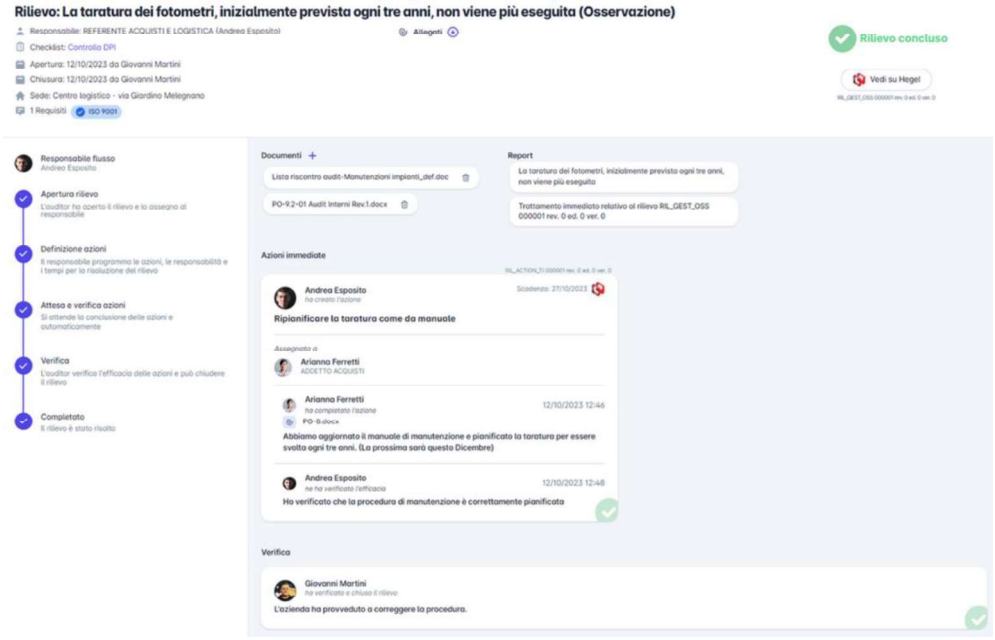
- **Contesto**: Analisi e gestione del contesto operativo e normativo.
- **Politica/obiettivi**: Definizione e monitoraggio delle politiche e degli obiettivi dell'organizzazione.
- **Rischi**: Identificazione e gestione dei rischi.
- **Checklist**: Creazione e gestione di checklist per varie attività.
- **Audit**: Gestione degli audit interni ed esterni.
- **Rilievi**: Documentazione e gestione dei rilievi.
- **Formazione**: Gestione dei programmi di formazione.
- **Competenze tecniche**: Gestione delle competenze tecniche del personale.
- **Alert**: Sistema di notifiche e allarmi per monitorare vari aspetti riferiti alla gestione delle norme.

Seguono alcune immagini relative alle APPLICAZIONI di KEYMAP:

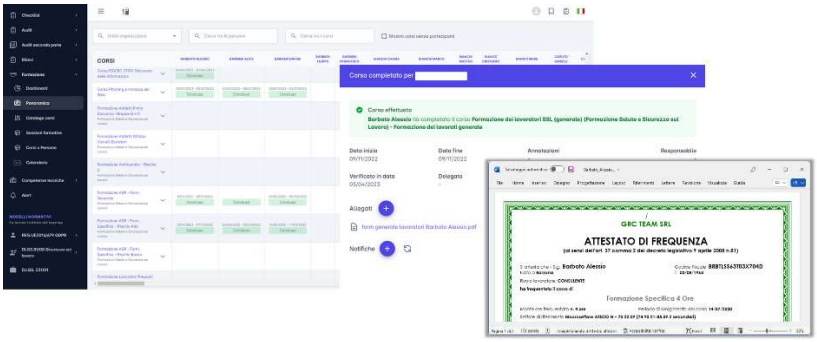
- **Gestione del Rischio**



- **Rilievi:** Non conformità, osservazioni, opportunità di miglioramento.



- **Formazione del Personale**



Modelli Normativi e Sistemi di Gestione richiesti

- **ISO 9001:2015**
- **ISO/IEC 27001:2022**
- **GDPR**

La piattaforma può integrare ulteriori norme di riferimento come Dlgs 81/08, Dlgs. 231/01, ISO 22301, ISO 37001, ISO/IEC 27701, ISO/IEC 27017, ISO/IEC 27018, ISO 14001, ISO 45001, e altre.

Infrastruttura Tecnologica

La piattaforma KEYMAP sarà installata presso il nostro Cloud in versione container con un numero massimo di cinque utenti, disponibile su Cloud Server Aruba in un datacenter TIER4 qualificato ACN (ex AGID).

Servizio Virtual Private Cloud e Scalabilità

Il servizio Virtual Private Cloud offre risorse di calcolo (vCPU, RAM, HD), di rete (VLAN, firewall, IP pubblici) e altri servizi (DRaaS, BaaS). Tramite VMware Cloud Director, è possibile creare e gestire data center virtuali con funzioni avanzate.

Servizio di Monitoraggio Infrastrutturale

Sistemi di monitoraggio continuo sorvegliano l'ambiente virtuale per rilevare problemi, disservizi o malfunzionamenti. Il monitoraggio delle risorse utilizzate (vCPU, RAM, HD, rete) permette di allertare il team di supporto in caso di superamento delle soglie.

Backup e Ripristino

Il servizio prevede un RPO (Recovery Point Objective) di 24 ore e un RTO (Recovery Time Objective) di 8 ore, garantendo la protezione e il rapido ripristino dei dati.

Separazione degli Ambienti di Sviluppo e Produzione

Gli ambienti di produzione e sviluppo sono separati e gestiti in modo indipendente, seguono procedure specifiche per garantire qualità, sicurezza ed efficienza delle applicazioni.

Sicurezza e Compliance

La piattaforma KEYMAP è sottoposta periodicamente a vulnerability assessment e penetration test per garantire la sicurezza e la protezione dei dati. La gestione integrata della mappatura delle informazioni e del registro dei trattamenti di dati personali è conforme alle best practice di secure coding (OWASP, NIST).

Servizio di assistenza e tempi di intervento

Il servizio di assistenza per la piattaforma KEYMAP è disponibile tramite email all'indirizzo support@imteam.it .

Se il Cliente non può utilizzare il servizio email, può contattare il servizio tecnico chiamando il numero 035 636029 e premendo il tasto "8" oppure tramite il numero verde 800608307. La registrazione della richiesta permette il rilascio di un ticket che identifica la chiamata e monitora l'avanzamento del lavoro. Tramite il numero di ticket, il Cliente potrà essere aggiornato sullo stato di risoluzione del problema segnalato.

Orari di Assistenza

L'assistenza è disponibile da lunedì a venerdì, dalle 8:30 alle 12:30 e dalle 13:30 alle 17:30. I giorni festivi, le due settimane centrali di agosto e gli interventi fuori orario lavorativo sono esclusi.

Tempi di Presa in Carico

La presa in carico della segnalazione è garantita entro 16 ore lavorative dalla richiesta. In caso di problematiche bloccanti, la presa in carico è garantita entro la mezza giornata lavorativa successiva alla richiesta.

4. Competenze ed esperienze

Requisiti di idoneità di GRCteam e di competenza professionale del team di lavoro

GRCteam fa parte di IMTEAM, un gruppo di sei aziende che unisce le singole competenze per generare valore grazie alla consulenza specializzata nella gestione dei processi aziendali e nello sviluppo di soluzioni digitali personalizzate.

In particolare, GRCteam opera dall'anno 2016 nell'ambito della consulenza nella gestione degli adempimenti normativi, nella progettazione, nello sviluppo e nel mantenimento dei sistemi di gestione in conformità agli standard internazionali e alle best practices di settore.

GRCteam è regolarmente iscritta al registro delle imprese presso la Camera di Commercio, Industria, Artigianato e Agricoltura (C.C.I.A.A.), specificatamente per i servizi oggetto della presente procedura.

GRCteam ha conseguito, ed è tuttora in corso validità, la certificazione del sistema di gestione per la qualità secondo la norma UNI EN ISO 9001.

GRCteam è in possesso della certificazione del sistema di gestione della sicurezza delle informazioni secondo le norme ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, e ha provveduto volontariamente alla nomina del DPO in ambito GDPR.

GRCteam include nel suo organico sette lead auditor certificati secondo la norma ISO/IEC 27001, cinque lead auditor certificati secondo la norma ISO 9001 e tre legali qualificati DPO.

Per tali attività GRCteam metterà a disposizione del cliente un team di lavoro dotato di tutte le competenze tecniche, informatiche, giuridiche e gestionali richieste.

Nel dettaglio le aree di competenza sono:

AREA DI COMPETENZA	OBIETTIVO	RUOLI E AMBITI
GESTIONALE-ORGANIZZATIVA	Supportare l'organizzazione nel comprendere il contesto di riferimento e implementare le attività necessarie attraverso metodologie e framework adeguatamente profilati.	Senior Consultant in ambito ISO/IEC 27001, ISO 9001, ISO 22301, GDPR Esperti in materia di integrazione di modelli normativi e sistemi di gestione
TECNOLOGICA	Identificare l'infrastruttura tecnologica, individuare gli adeguamenti, i presidi di controllo, le modalità e frequenze di monitoraggio necessari al fine di proteggere il patrimonio informativo dalle minacce che possano compromettere la sicurezza delle informazioni	IT – Soluzioni web & cloud - Project Management, Architetture IT, Strategia Tecnologica, IT Project Management IT – Soluzioni desktop - COBIT, ITIL, GDPR IT Security lead auditor e auditor Business Continuity/Disaster Recovery Plans consultant
LEGALE	Verificare le implicazioni in materia di sicurezza delle informazioni nella documentazione contrattuale; garantire che il modello costruito sia effettivamente idoneo in relazione ai requisiti della norma ISO (tenendo conto delle implicazioni e degli impatti con gli altri temi di compliance)	Consulente legale su temi di contrattualistica Data Protection Officer (DPO) Senior Consultant GDPR