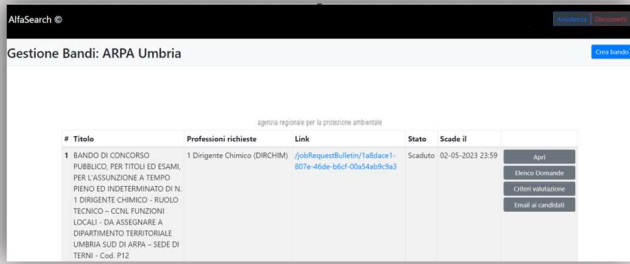


	Tipo documento	Applicativo	Codice Doc.	Data doc.
	Scheda tecnica software	AlfaSearch	SPECS3/2024	12/02/2024

A) Requisiti e caratteristiche tecniche del software

Cod.	Tipo	Descrizione
A.1	Nome del software	AlfaSearch
A.2	Release	2.0
A.3	Tipologia	Software Gestionale
A.4	Layout applicativo	
A.5	Campo di applicazione	Il servizio AlfaSearch offre la possibilità alle Aziende del SSN di gestire le attività rese in regime di prestazioni aggiuntive.
A.6	Modalità di erogazione	SaaS
A.7	Infrastruttura IaaS	Aruba S.p.a
A.8	Licenza	Multi-tenant
A.9	Versione	Web
A.10	Compatibilità con i browser	Su tutti i browser più popolari, ottimizzato per il funzionamento con Google Chrome
A.11	Sistema Operativo Client	Qualsiasi sistema operativo in cui sia installabile un browser compatibile
A.12	Lingua	Italiano
A.13	Contenuti accessori	Manuali d'uso della procedura
A.14	Architettura	AlfaSearch adotta un'architettura a 3 livelli: il Presentation Layer è costituito da file HTML, CSS e JS che definiscono l'interfaccia utente dell'applicativo. Il Middle Layer, ospitato su Web Server Nginx, incorpora la Business Logic ed è implementato attraverso componenti Python 3 e Django per il data service e il transaction management. Il Data Layer si basa su un database PostgreSQL. Non viene utilizzato alcun cookie tracciante.
A.15	Informazioni sull'utilizzo	AlfaSearch è un'applicazione SaaS distribuita come Applicazione Web; è sufficiente avere un browser compatibile sul dispositivo client e una connessione internet per utilizzarla.
A.16	Autenticazione e cambio password	L'accesso ad Alfa Search avviene con chiavi username e password, attraverso credenziali SPID. Per l'amministratore del servizio è previsto l'accesso tramite e-mail aziendale. La password viene scelta in base ai criteri di robustezza. Se richiesto può essere attivato il servizio di autenticazione SPID. Sono presenti differenti livelli di accesso a secondo delle autorizzazioni degli utenti: Amministratore e utente
A.17	Caching e performance	Viene eseguito il caching dei file Web nella cache del browser per ottimizzare gli accessi successivi. L'utilizzo di protocolli di tipo Ajax riduce il traffico di rete. Il caching dei dati sul server consente di ottimizzare l'accesso al database, basandosi su connection pooling.
A.18	Installazione presso il cliente	Non prevista
A.19	Amministratori di sistema	Personale HMS Consulting

	Tipo documento	Applicativo	Codice Doc.	Data doc.
	Scheda tecnica software	AlfaSearch	SPECS3/2024	12/02/2024

B) Requisiti e caratteristiche di sicurezza

Cod.	Tipo	Descrizione
B.1	Sistemi di crittografia	Tutti i dati trasferiti tra il client e il server HMS Consulting protocollo HTTPS in modo da essere compatibile con corporate firewall.
B.2	Patching	Sistema operativo e componenti di terze parti periodicamente aggiornati
B.3	Vulnerability assesment	Penetration test pubblicato periodicamente all'interno del sito: https://www.hmsconsulting.it/doc
B.3	Vulnerability assesment Protocolli adottati	Standard Top 10 O.W.A.S.P.
B.4	Controllo degli accessi	Gli accessi vengono monitorati dall'amministratore di sistema
B.5	Meccanismi di sicurezza	Sono applicati time-out di sessione
B.6	Protezione dati	I dati aziendali sono protetti mediante backup giornaliero (alle ore 4.00 a.m.), settimanale e mensile con retention di 60 giorni. Le copie sono distribuite in Cloud presso Aruba S.P.A. e allocati in ambienti diversi rispetto agli ambienti di produzione. Policy aggiuntive sono implementabili dietro esplicita richiesta del cliente.
B.7	Misure di sicurezza applicabili su richiesta	Opzionalmente può essere attivata autenticazione a due fattori (MFA) registrando un numero telefonico.
B.8	Trattamento Dati	L'infrastruttura informatica <i>IaaS</i> dell'applicativo è ubicata in Italia, i dati sono trattati e conservati secondo le normative vigenti UE GDPR 2016/679 e codice Privacy 196/2003 per un periodo di 6 mesi al termine dei quali saranno cancellati. Hms assicura la riservatezza, integrità e disponibilità dei dati per cui è nominata come responsabile. Il Responsabile esterno del trattamento dati è Francesco Lorenzini nella persona del legale rappresentate di HMS Consulting S.r.l.; Le aree interne al software che trattano "dati personali particolari sono evidenziate" con specifica dicitura.
B.9	Cancellazione dei dati	Di seguito la procedura di cancellazione dei dati attuata da HMS: 1)Una volta decadute le finalità giuridiche del trattamento, HMS notificherà al cliente la cancellazione dei dati e dunque, su richiesta del cliente, provvederà ad una modalità di restituzione degli stessi. 2)Dopo 6 mesi dal termine di contratto HMS provvederà alla cancellazione dei dati effettuando una cancellazione di terzo livello attraverso un software che permette la distruzione sicura dei file ".db" e delle copie di backUp.
B.10	Tutela della proprietà intellettuale	AlfaSearch è di proprietà di HMS Consulting e ne vieta l'uso non autorizzato se non attraverso la specifica licenza. Tutti i componenti software di terze parti utilizzati all'interno dell'applicativo sono impiegati rispettando i diritti di proprietà intellettuale attraverso l'acquisizione della licenza.
B.11	Linee guida di riferimento	Alfa Search è sviluppato, monitorato e protetto secondo le linee guida di riferimento per quanto riguarda la sicurezza delle informazioni ISO/IEC 27001:2022 e 27017/27018 per la sicurezza servizi cloud e le PII contenute.
B.12	Sincronizzazione degli orologi	Gli orologi sono sincronizzati da protocollo NTP.

C) Assistenza tecnica

Cod.	Tipo	Descrizione
C.1	Servizio assistenza tecnica	Il tipo di assistenza tecnica e i relativi canali di contatto possono variare a seconda del contratto stipulato. Disponibilità*: Dal lunedì al venerdì dalle 9:00 alle 13:00 e dalle 14:30 alle 18:00. *Eventuali riduzioni di orario saranno consentite nel periodo 24/12 e 6/1 e a cavallo di Ferragosto e comunque concordandolo antecedentemente con gli uffici.
C.2	Canali di assistenza tecnica utenti	-e-mail: helpdesk@hmsconsulting.it ; -n° telefonico dedicato;

	Tipo documento	Applicativo	Codice Doc.	Data doc.
	Scheda tecnica software	AlfaSearch	SPECS3/2024	12/02/2024

		-Sistema di ticketing Jira;								
C.3	Canale segnalazione violazione privacy	In caso in cui il cliente fosse coinvolto in incidenti di violazione della privacy o incedenti al sistema di sicurezza informatica deve contattare i nostri uffici al seguente indirizzo: -hmsconsulting@pec.it -dpo@hmsconsulting.it								
C.4	Manutenzione applicativo	Il servizio di manutenzione sarà organizzato al fine di garantire la manutenzione preventiva/ordinaria e la manutenzione correttiva della procedura e non intaccare le normali attività.								
C.5	Monitoraggio	Gli amministratori di sistema di HMS effettuano i monitoraggi periodici dell'applicativo relativamente alle capacità delle risorse (CPU, RAM) e accessi al sistema non autorizzati e traffico Broadcast; I clienti possono richiedere informazioni specifiche al riguardo; HMS si impegna a fornire i risultati dei monitoraggi effettuati. Nel caso in cui si verificassero situazioni anomale e/o violazione di dati che coinvolge dati personali sarà cura di HMS avvisare il cliente, riportando tutte le circostanze degli eventi.								
C.6	Canali di disservizio dell'applicativo	In caso di disservizio il cliente potrà contattare gli uffici tecnici di HMS al seguente indirizzo e-mail: helpdesk@hmsconsulting.it descrivendo la problematica riscontrata. Hms si riserva di effettuare un'analisi preventiva per la valutazione e nel caso di errore bloccante i tempi di ripristino sono definiti all'interno dei livelli di servizio.								
C.7	Service Level Agreement (SLA)	Hms garantisce i seguenti livelli di servizio dell'applicativo: <table border="1" data-bbox="550 840 1428 1048"> <thead> <tr> <th>Parametro</th> <th>SLA tempo di risposta</th> </tr> </thead> <tbody> <tr> <td>Tempo di presa in carico per disservizi definiti bloccanti e critici</td> <td>Entro 2 ore dalla 1° segnalazione</td> </tr> <tr> <td>Tempo di presa in carico per disservizi definiti non bloccanti</td> <td>Entro 4 ore dalla 1° segnalazione</td> </tr> <tr> <td>Tempo di presa in carico per disservizi definiti non bloccanti e non critici</td> <td>Entro 1 giorno dalla 1° segnalazione</td> </tr> </tbody> </table>	Parametro	SLA tempo di risposta	Tempo di presa in carico per disservizi definiti bloccanti e critici	Entro 2 ore dalla 1° segnalazione	Tempo di presa in carico per disservizi definiti non bloccanti	Entro 4 ore dalla 1° segnalazione	Tempo di presa in carico per disservizi definiti non bloccanti e non critici	Entro 1 giorno dalla 1° segnalazione
Parametro	SLA tempo di risposta									
Tempo di presa in carico per disservizi definiti bloccanti e critici	Entro 2 ore dalla 1° segnalazione									
Tempo di presa in carico per disservizi definiti non bloccanti	Entro 4 ore dalla 1° segnalazione									
Tempo di presa in carico per disservizi definiti non bloccanti e non critici	Entro 1 giorno dalla 1° segnalazione									
C.8	Ruoli e responsabilità	HMS ha definito all'interno della propria organizzazione i ruoli e le responsabilità di gestione dell'applicativo. E' presente un team di unità di crisi che si attiverà nel caso in cui si verificassero le problematiche di cui al punto C.9. HMS assicura il funzionamento e la protezione dell'applicativo da malware, oltre che a verificare i diritti di accesso del proprio personale a tali risorse. Obblighi dell'Utente: Per quanto concerne la gestione degli ID utenti, sarà responsabilità degli utenti del cliente mantenere la riservatezza delle chiavi di accesso all'applicativo. HMS non è responsabile per eventuali incidenti derivanti da una gestione delle chiavi di accesso o da un uso non conforme alle policy stabilite. -L'Utente è tenuto a rispettare, e non può aggirare, le limitazioni tecniche del Prodotto, descritte nella manualistica. -L'Utente è tenuto a rispettare tutte le leggi e le normative applicabili al proprio utilizzo del Prodotto, incluse, tra le altre, tutte le leggi applicabili in materia di privacy, dati personali, protezione dei dati e riservatezza delle comunicazioni. È responsabilità dell'Utente rispondere a qualsiasi richiesta di terzi relativa all'utilizzo del Prodotto da parte dell'Utente stesso. - L'Utente non può vendere, noleggiare, concedere in leasing o prestare il Prodotto e/o il Software gestito a terzi né utilizzare il Prodotto per creare propri prodotti o servizi. - L'Utente non può rimuovere o modificare gli avvisi sul copyright, né altre note di proprietà del Prodotto, documenti o materiali correlati. - L'Utente non può verificare, valutare o testare la vulnerabilità del Prodotto o del Portale o di sistemi o reti correlati, né violare le misure di sicurezza o le procedure di controllo applicate in relazione al Prodotto, al Portale e a detti sistemi e reti. - Se l'Utente viola uno qualsiasi degli obblighi descritti di seguito o le limitazioni di licenza contenuti nel presente Contratto o in un altro documento legalmente vincolante stipulato HMS è autorizzata a revocare la licenza e disabilitare l'uso del Prodotto.								

C.9	Procedure di continuità operativa e gestione vulnerabilità'	<table border="1"> <thead> <tr> <th>N° Piano</th> <th>Evento</th> <th>Piano di continuità operativa</th> <th>Punto di Ripristino di default (PTO)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Disservizio critico al SaaS AlfaSearch</td> <td>a) Isolamento server e migrazione su nuovo; c) Recupero backup; d) installazione e configurazione macchina; e) Cambio DNS e comunicazione agli uffici preposti del cliente dell'avvenuto incidente;</td> <td>Back up del giorno prima</td> </tr> <tr> <td>2</td> <td>Disservizio infrastruttura IaaS di AlfaSearch</td> <td>Si fa riferimento alle procedure del fornitore dell'infrastruttura IaaS</td> <td>Back up del giorno prima</td> </tr> <tr> <td>3</td> <td>Data Breach</td> <td>a) Segnalazione dell'evento entro 72 H all'autorità per la protezione dei dati DPA (nel caso di violazione ad alto rischio); b) comunicazione tempestiva agli utenti e agli uffici preposti del cliente; c) In alcuni casi è previsto il blocco di accesso al sistema coinvolto con attuazione del piano 1.</td> <td>Back up del giorno prima</td> </tr> </tbody> </table>	N° Piano	Evento	Piano di continuità operativa	Punto di Ripristino di default (PTO)	1	Disservizio critico al SaaS AlfaSearch	a) Isolamento server e migrazione su nuovo; c) Recupero backup; d) installazione e configurazione macchina; e) Cambio DNS e comunicazione agli uffici preposti del cliente dell'avvenuto incidente;	Back up del giorno prima	2	Disservizio infrastruttura IaaS di AlfaSearch	Si fa riferimento alle procedure del fornitore dell'infrastruttura IaaS	Back up del giorno prima	3	Data Breach	a) Segnalazione dell'evento entro 72 H all'autorità per la protezione dei dati DPA (nel caso di violazione ad alto rischio); b) comunicazione tempestiva agli utenti e agli uffici preposti del cliente; c) In alcuni casi è previsto il blocco di accesso al sistema coinvolto con attuazione del piano 1.	Back up del giorno prima
		N° Piano	Evento	Piano di continuità operativa	Punto di Ripristino di default (PTO)													
		1	Disservizio critico al SaaS AlfaSearch	a) Isolamento server e migrazione su nuovo; c) Recupero backup; d) installazione e configurazione macchina; e) Cambio DNS e comunicazione agli uffici preposti del cliente dell'avvenuto incidente;	Back up del giorno prima													
		2	Disservizio infrastruttura IaaS di AlfaSearch	Si fa riferimento alle procedure del fornitore dell'infrastruttura IaaS	Back up del giorno prima													
3	Data Breach	a) Segnalazione dell'evento entro 72 H all'autorità per la protezione dei dati DPA (nel caso di violazione ad alto rischio); b) comunicazione tempestiva agli utenti e agli uffici preposti del cliente; c) In alcuni casi è previsto il blocco di accesso al sistema coinvolto con attuazione del piano 1.	Back up del giorno prima															