


	Tipo documento	Applicativo	Codice Doc.	Data doc.
	Scheda tecnica software	AlfaPlus	SPECS2/2024	12/02/2024

## A) Requisiti e caratteristiche tecniche del software

Cod.	Tipo	Descrizione
A.1	Nome del software	AlfaPlus
A.2	Release	4.1.2
A.3	Tipologia	Software Gestionale
A.4	Layout applicativo	
A.5	Campo di applicazione	Il servizio AlfaPlus 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	Single 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	AlfaPlus 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	AlfaPlus 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	<p>L'accesso ad AlfaPlus avviene con chiavi username e password. L'username può corrispondere alla e-mail aziendale. La password viene scelta in base ai criteri di robustezza. Ciascun utente può cambiare la password di accesso in autonomia, previa ricezione di una mail con link di ripristino.</p> <p>Sono presenti differenti livelli di accesso a secondo delle autorizzazioni degli utenti.</p> <ol style="list-style-type: none"> <li>1) Controller</li> <li>2) Super-manager</li> <li>3) Operation manager</li> <li>4) Utente</li> </ol> <p>Gli utenti non possono iscriversi in autonomia al sito, ma previa specifica richiesta dell'azienda cliente agli amministratori di sistema, i quali effettueranno le attivazioni secondo i privilegi attribuiti.</p> <p>L'azienda cliente si assume la responsabilità di richiedere l'elenco delle utenze attive/disattive al fine di richiederne la modifica o la cancellazione agli amministratori di sistema.</p>
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. Per il corretto funzionamento del collegamento verificare l'apertura delle porte http (80) e https (443).

	Tipo documento	Applicativo	Codice Doc.	Data doc.
	Scheda tecnica software	AlfaPlus	SPECS2/2024	12/02/2024

A.19	Amministratori di sistema	Personale HMS Consulting
------	---------------------------	--------------------------

## 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 fanno uso esclusivo di protocollo HTTPS.
B.2	Patching	Sistema operativo e componenti di terze parti periodicamente aggiornati
B.3	Vulnerability assesment	Penetration test pubblicato periodicamente all'interno del sito: <a href="https://www.hmsconsulting.it/doc">https://www.hmsconsulting.it/doc</a> Saranno gestiti tutti i risultati del test categorizzati come "high".
B.3	Vulnerability assesment Protocolli adottati	Protocollo Top 10 O.W.A.S.P.
B.4	Controllo degli accessi	Vengono effettuati controlli periodici degli accessi al sistema tramite LOG.
B.5	Meccanismi di sicurezza	Sono applicati time-out di sessione
B.6	Protezione dati	Antivirus di sistema Rootkit Hunter. I dati aziendali sono protetti mediante backup full giornaliero (alle ore 4.00 pm), settimanale e mensile con retention di 60 giorni. Le copie sono distribuite sia in Cloud presso Aruba S.p.a e sono 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. Durante il periodo di archiviazione, i dati vengono conservati in ambienti informatici distinti da quelli di produzione. L'accesso è consentito esclusivamente al personale autorizzato, tramite credenziali protette da password. Inoltre, tali ambienti sono soggetti a rigorosi controlli di tracciamento degli accessi (log). 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.;
B.9	Cancellazione dei dati	Di seguito la procedura di cancellazione dei dati attuata da HMS:  <ol style="list-style-type: none"> <li>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.</li> <li>2) Dopo 6 mesi dal termine di contratto, HMS provvederà alla cancellazione dei dati effettuando una cancellazione di terzo livello attraverso un software che consente la distruzione sicura dei file ".db" e delle copie di backup, garantendo l'eliminazione irreversibile delle informazioni mediante tecnica di sovrascrittura a che ne impedisce il recupero anche con strumenti avanzati.</li> </ol>
B.10	Tutela della proprietà intellettuale	AlfaPlus 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 di sviluppo	AlfaPlus è sviluppato, monitorato e protetto in conformità con le linee guida ISO/IEC 27001:2022 per la sicurezza delle informazioni, nonché con ISO/IEC 27017 e 27018 per la sicurezza dei servizi cloud e le PII contenute. E' certificato ACN ID scheda: SA-4364

	Tipo documento	Applicativo	Codice Doc.	Data doc.
	Scheda tecnica software	AlfaPlus	SPECS2/2024	12/02/2024

B.12	Sincronizzazione degli orologi	Gli orologi sono sincronizzati tramite 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: <a href="mailto:helpdesk@hmsconsulting.it">helpdesk@hmsconsulting.it</a> ; -n° telefonico dedicato;								
C.3	Canale segnalazione violazione privacy	In caso in cui il cliente fosse coinvolto in incidenti di violazione della privacy o incidenti al sistema di sicurezza informatica deve contattare i nostri uffici al seguente indirizzo: -hmsconsulting@pec.it <a href="mailto:dpo@hmsconsulting.it">-dpo@hmsconsulting.it</a>								
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 hardware (CPU, RAM) e accessi al sistema non autorizzati; 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: <a href="mailto:helpdesk@hmsconsulting.it">helpdesk@hmsconsulting.it</a> 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: <table border="1" data-bbox="555 1279 1394 1491"> <thead> <tr> <th>Parametro SLA</th> <th>RTO</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 disservizi definiti non bloccanti e non critici</td> <td>Entro 1 giorno dalla 1° segnalazione</td> </tr> </tbody> </table>	Parametro SLA	RTO	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 disservizi definiti non bloccanti e non critici	Entro 1 giorno dalla 1° segnalazione
Parametro SLA	RTO									
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 disservizi definiti non bloccanti e non critici	Entro 1 giorno dalla 1° segnalazione									
C.8	Ruoli e responsabilità degli utenti	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.								

	<b>Tipo documento</b>	<b>Applicativo</b>	<b>Codice Doc.</b>	<b>Data doc.</b>
	<b>Scheda tecnica software</b>	AlfaPlus	SPECS2/2024	12/02/2024

		<p>- 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.</p> <p>- L'Utente non può rimuovere o modificare gli avvisi sul copyright, né altre note di proprietà del Prodotto, documenti o materiali correlati.</p> <p>- 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.</p> <p>- 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.</p>																
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 (RPO)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Disservizio critico al SaaS AlfaPlus</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 (24 h)</td> </tr> <tr> <td>2</td> <td>Disservizio infrastruttura IaaS di AlfaPlus</td> <td>Si fa riferimento alle procedure del fornitore dell'infrastruttura IaaS</td> <td>Back up del giorno prima (24 h)</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 (24 h)</td> </tr> </tbody> </table>	N° Piano	Evento	Piano di continuità operativa	Punto di Ripristino (RPO)	1	Disservizio critico al SaaS AlfaPlus	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 (24 h)	2	Disservizio infrastruttura IaaS di AlfaPlus	Si fa riferimento alle procedure del fornitore dell'infrastruttura IaaS	Back up del giorno prima (24 h)	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 (24 h)
N° Piano	Evento	Piano di continuità operativa	Punto di Ripristino (RPO)															
1	Disservizio critico al SaaS AlfaPlus	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 (24 h)															
2	Disservizio infrastruttura IaaS di AlfaPlus	Si fa riferimento alle procedure del fornitore dell'infrastruttura IaaS	Back up del giorno prima (24 h)															
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 (24 h)															