

ALLEGATO 2

CAPITOLATO TECNICO

**Appalto Specifico indetto da Consip S.p.A. per
l'acquisizione della soluzione SAP CDC per Sogei
ID – 2925**

INDICE

1	PREMESSA	4
1.1	DEFINIZIONI	4
1.2	LINGUA	5
1.3	RISERVATEZZA	5
2	CONTESTO TECNICO-ORGANIZZATIVO	7
3	OGGETTO DELLA FORNITURA	9
4	CARATTERISTICHE DELLA FORNITURA	10
4.1	SAP CDC – SUPPORTO OPERATIVO DELLE COMPONENTI LEGACY IN FASE DI SETUP	10
4.2	SAP CDC – DIRITTO D'USO DEL SOFTWARE	13
4.3	SAP CDC – INFRASTRUTTURA	16
4.3.1	<i>Architettura logica SAP CDC</i>	16
4.3.2	<i>Architettura di integrazione di rete e SAN</i>	17
4.3.3	<i>Piattaforme SAP in ambito</i>	18
4.3.4	<i>System Landscape / Sizing</i>	20
4.4	SAP CDC – SERVIZI	31
4.4.1	<i>Servizi di gestione della SAP CDC</i>	31
4.4.1.1	SAP Technical Managed Services	33
4.4.1.2	SAP Enhanced Operations Services	34
4.4.1.3	Servizi tecnico/applicativi aggiuntivi	36
4.4.1.4	Servizi aggiuntivi a copertura di eventuali richieste al momento non pianificabili	39
4.4.2	<i>Servizi Specialistici SAP Premium Engagement/Quality Assurance</i>	39
4.5	SAP CDC – SPECIFICITÀ DEL SERVIZIO SOGEI	43
4.5.1	<i>SAFEKEEPER - estensione finestra gestione per sistemi S/4HANA su SAP CDC</i>	43
4.5.2	<i>DISASTER RECOVERY</i>	43
4.5.3	<i>LOGGING / AUDITING</i>	44
4.5.4	<i>MONITORAGGIO CDC e STRUMENTI A SUPPORTO DELLE OPERATION</i>	44
4.5.5	<i>IAAS logs, VM per attività day-by-day</i>	46
4.5.6	<i>BACKUP</i>	48
4.5.7	<i>SCHEDULAZIONE DEI JOB</i>	48
4.5.8	<i>VULNERABILITY ASSESSMENT</i>	49
4.5.9	<i>GESTIONE INCIDENTI DI SICUREZZA</i>	49
4.5.10	<i>PROCEDURA SERVICE CONTINUITY PLAN</i>	49
4.5.11	<i>ENCRYPTION</i>	51
4.5.12	<i>ACCESSO AL DATO IN SAP CDC</i>	52
4.5.13	<i>Gestione lifecycle utenza SAPHANADB</i>	55
4.6	SOFTWARE LIFECYCLE INDUSTRIALIZZATO	56
4.7	SAP SAC - SAP ANALYTICS CLOUD (POST SETUP)	57
4.8	SAP BTP - BUSINESS TECHNOLOGY PLATFORM (POST SETUP)	57
4.9	MANUTENZIONE ON PREMISE RESIDUA	57

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

4.10	ALTRI REQUISITI DELLA FORNITURA.....	60
4.10.1	<i>Certificazioni della soluzione CDC</i>	60
4.10.2	<i>Qualifica ACN</i>	60
4.10.3	<i>Cybersicurezza - DPCM del 15 giugno 2021</i>	60
4.10.4	<i>Cybersicurezza - DPCM del 30 Aprile 2025</i>	67
4.11	PIANIFICAZIONE DELL'ATTIVITÀ DI MOVING	67
4.11.1	<i>PREPARAZIONE – ATTIVITÀ PRELIMINARI ALL'ATTIVAZIONE SAP CDC</i>	70
4.11.2	<i>ESECUZIONE – ATTIVITÀ PER LA MIGRAZIONE DELLE PIATTAFORME IN SAP CDC</i>	72
4.11.2.1	<i>S/4HANA MOVE E SPLIT CONTESTUALE</i>	73
4.11.2.2	<i>BW/4HANA UPGRADE on Premise</i>	73
4.11.2.3	<i>APPROCCIO GREENFIELD CON MIGRAZIONE APPLICATIVA SAP BO</i> ...	74
4.11.2.4	<i>MOVE ALTRI SISTEMI SAP</i>	74
5	DURATA E SEDE DELLA FORNITURA	75
6	MODALITÀ DI ESECUZIONE DELLA FORNITURA.....	77
6.1	CONSEGNA, INSTALLAZIONE E CONFIGURAZIONE DELLA SOLUZIONE	77
6.2	EROGAZIONE DEL SERVIZIO DI MANUTENZIONE.....	78
6.3	EROGAZIONE DEI SERVIZI DI SUPPORTO SPECIALISTICO.....	80
6.3.1	<i>Approvazione e sostituzione delle figure professionali</i>	80
6.4	RESPONSABILE DELLA FORNITURA E MODALITÀ DI COMUNICAZIONE.....	81
7	VERIFICA DI CONFORMITÀ	83
7.1	TEST CVCN.....	85
8	PORTALE FORNITORI.....	87
8.1	ACCREDITAMENTO DEL PERSONALE.....	87
	ALLEGATO 1 – LINEE GUIDA SERVICE CONTINUITY PLAN	88

1 PREMESSA

Il presente documento riguarda l'acquisizione, per la Sogei S.p.A., di un nuovo modello di attivazione e di fruizione delle soluzioni e dei servizi SAP in grado di soddisfare tempestivamente la crescita di utenze legata all'adozione dell'applicativo nonché rafforzare le modalità di gestione della piattaforma SAP e garantire la continuità di servizio per quelle componenti a sottoscrizione cloud in un'ottica di razionalizzazione e ottimizzazione complessiva dei costi.

L'acquisizione, inoltre, comprende il rinnovo del servizio di manutenzione per quelle componenti che non saranno trasportate all'interno del nuovo modello nonché il rinnovo di alcune delle soluzioni di cloud pubblico SAP ad oggi in uso presso l'Amministrazione.

1.1 Definizioni

Salvo diversa esplicita indicazione, ai termini riportati di seguito, viene attribuito, ai fini del presente Capitolato e del Contratto (di cui il presente documento costituisce parte integrante), il significato di seguito indicato:

- **Consip:** la società che, in qualità di stazione appaltante della presente fornitura, affida la fornitura oggetto del presente Capitolato;
- **Sogei:** la Società Generale di Informatica s.p.a., beneficiaria della fornitura (anche "*Committente*");
- **RGS:** la Ragioneria Generale dello Stato;
- **MEF:** Ministero dell'Economia e delle Finanze;
- **Amministrazione:** Per Amministrazione si intende il Ministero dell'Economia e delle Finanze, che è proprietario dell'intero capitale di Sogei, con riferimento alle proprie strutture organizzative destinatarie dei servizi erogati dalla Sogei sia attraverso infrastrutture proprietarie che attraverso infrastrutture proprietarie delle singole strutture organizzative; rientrano nella presente definizione le altre Amministrazioni, ivi compresi gli Enti e le Società pubbliche per cui Sogei svolge e/o svolgerà, per disposizione legislativa o amministrativa, (decreto ministeriale, decreto di natura normativa o decreto presidenza consiglio dei ministri), ogni altra attività di natura informatica;
- **Impresa/Fornitore:** la società affidataria della fornitura;
- **Capitolato tecnico:** il presente documento che enuncia le specifiche tecniche alle quali si dovrà conformare la fornitura;
- **Contratto:** il contratto che verrà stipulato tra la Sogei e l'Impresa che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura;
- **Data di accettazione:** La data della verifica di conformità con esito positivo della

fornitura e di conseguente accettazione della fornitura, da cui decorre la durata contrattuale;

- **Data di consegna:** La data di ricezione della PEC contenente le indicazioni per scaricare il software e le informazioni per usufruire del servizio di software assurance ovvero nel caso di fruizione di software in modalità “cloud”;
- **SAP CDC:** si intende il servizio SAP Rise with “SAP Private Tailored Option, Customer Data Center” altresì nominato “SAP Cloud ERP Private, tailored option”, comprendente l’elenco delle componenti software, gli aspetti tecnici e di *sizing*, l’elenco dei servizi tecnico/applicativi ricompresi all’interno della sottoscrizione;
- **SAP PE:** servizi SAP di premium engagement;
- **SAP BTP:** Soluzione SAP *Business Technology Platform*;
- **SAP SAC:** Soluzione SAP *Analytics Cloud*;
- **Fornitura:** il complesso delle attività oggetto del presente Capitolato tecnico;
- **Noleggio (o ‘subscription’):** indica la modalità di concessione delle Licenze in uso a tempo determinato, con le modalità indicate nel presente Capitolato;
- **Malfunzionamento:** qualsiasi anomalia funzionale del software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d’uso;
- **Responsabile della Fornitura:** la persona individuata dall’Impresa come interlocutore di SOGEI e responsabile di tutte le attività contrattuali.
- **Direttore dell’esecuzione:** la persona, individuata da Sogei come interlocutore tecnico dell’Impresa per tutte le attività contrattuali.
- **Software vendor SAP:** la società proprietaria dei prodotti oggetto dell’appalto.

1.2 Lingua

La lingua utilizzata per tutte le attività e la documentazione relative al presente contratto d’appalto sarà la lingua italiana.

1.3 Riservatezza

Tutte le informazioni trattate e tutti i documenti, anche parziali, scambiati tra l’Impresa e la Committente nell’ambito dell’esecuzione del presente contratto d’appalto sono riservati; pertanto, è richiesta la massima cautela nel loro utilizzo, in particolare laddove questo avvenga al di fuori delle sedi della Committente.

L'Impresa, al di fuori delle attività oggetto del presente contratto d'appalto, non potrà utilizzare, a nessun titolo, la documentazione e i moduli software acquisiti da Sogei o prodotti specificatamente per i servizi oggetto del presente Capitolato Tecnico.

2 CONTESTO TECNICO-ORGANIZZATIVO

L'oggetto della presente procedura è l'acquisizione della soluzione SAP CDC per Sogei.

Sogei, in qualità di partner tecnologico istituzionale della Ragioneria Generale dello Stato, svolge un ruolo strategico nella progettazione, realizzazione e gestione dei sistemi informativi a supporto delle sue funzioni essenziali, garantendo continuità, affidabilità e coerenza evolutiva alle soluzioni adottate. In tale contesto, la SOGEI garantisce, in modo continuativo, elevati livelli di servizio, performance applicative adeguate e piena affidabilità operativa, in risposta a un fabbisogno diffuso in costante evoluzione.

In questo contesto, le piattaforme SAP, sia quelle ricomprese nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC) sia quelle ritenute strategiche con specifico riferimento alla funzione essenziale del Bilancio dello Stato e alla gestione e monitoraggio dei Fondi Europei relativi al Piano Nazionale Ripresa e Resilienza, al Piano complementare e ai programmi dei Fondi strutturali della programmazione 2014-2020 nonché del cofinanziamento nazionale, servono attualmente una platea di oltre 60.000 utenti, distribuiti tra numerose articolazioni dello Stato e diversi enti pubblici nonché degli enti di controllo della Commissione Europea.

Le soluzioni SAP sono state adottate per la realizzazione di progettualità di primaria importanza utilizzate dalla divisione Economia e dalla divisione Finanze a supporto di servizi critici, quali:

- Programma INIT per il rifacimento dei sistemi di finanza pubblica;
- Progetto Regis a supporto del Piano Nazionale di Ripresa e Resilienza ed a tendere della Programmazione europea;
- Sistema Finanziario IGRUE;
- Progetto Ortes;
- Piattaforma BDAP per la fruizione da parte delle Amministrazioni Pubbliche dei dati della Finanza Pubblica;
- Sistemi di reportistica e visualizzazione dati basati su Business Object (BO) per:
 - Progetto Tessera Sanitaria;
 - Progetto Area RGS;
 - Progetto DWHRGS.

Per la divisione Economia (Dipartimento degli Affari Generali) i prodotti SAP BO sono utilizzati per il Progetto Service Personale Tesoro e NoiPA.

I Sistemi di reportistica e visualizzazione dati basati su Business Object (BO) sono utilizzati inoltre dall'Agenzia della Coesione Territoriale (nel seguito ACT) e da Sogei per altri clienti.

Nell'ambito delle linee di attività di evoluzione ed innovazione delle tecnologie a supporto dei processi RGS, Sogei ha deciso di adottare un nuovo modello di attivazione e di fruizione delle soluzioni e dei servizi SAP. Il nuovo modello ha come elemento centrale l'adozione del servizio gestito SAP CDC; l'attivazione del servizio richiederà circa 6 mesi di preparazione dalla firma del contratto.

La soluzione consente, in continuità con quanto realizzato sino ad oggi, di rinnovare lo strato tecnologico ed applicativo, adottando all'interno dei Data Center Sogei una soluzione unica progettata, testata ed ingegnerizzata da SAP in modo integrato. Nel rispetto degli obiettivi della Committente, l'attivazione della SAP CDC dovrà avvenire entro e non oltre il 30 giugno 2026, o diverso termine eventualmente concordato con Sogei.

3 OGGETTO DELLA FORNITURA

La presente procedura di gara ha ad oggetto l'acquisizione di:

- **soluzione SAP CDC**, soluzione ingegnerizzata SAP ottimizzata in fase di progettazione e di test, replicabile secondo standard predefiniti per garantire prestazioni elevate, affidabilità e semplicità di gestione e comprendente al suo interno:
 - **SetUP**. La soluzione includerà la transizione graduale verso il nuovo modello SAP CDC, dove il software vendor dovrà garantire la continuità operativa dei servizi erogati dal sistema *legacy*. In questa fase, il software vendor dovrà garantire la piena operatività delle componenti *legacy*, assicurando la stabilità complessiva dell'ambiente durante il periodo di setup.
 - **SW**. Il modello SAP CDC includerà il diritto d'uso delle componenti software ad oggi in uso da Sogei e oggetto di evoluzione verso la nuova soluzione, considerando anche le eventuali variazioni dei volumi legate ai nuovi fabbisogni.
 - **HW**. Il modello SAP CDC includerà il comodato d'uso delle infrastrutture tecniche sottostanti le applicazioni software che saranno installate all'interno dei Data Center Sogei.
 - **Servizi Specialistici**. Il modello SAP CDC, in quanto servizio gestito, prevederà l'erogazione dei servizi tecnici di gestione e supporto (Servizi SAP tecnico applicativi della CDC, SAP Premium Engagement / Quality Assurance e Servizi Addizionali SAP).
 - **Software Lifecycle industrializzato**. A completamento del modello, sarà inclusa nel SAP CDC una soluzione di *Software Lifecycle* industrializzato.
- Servizio SAP SAC – *SAP Analytics Cloud*.
- Servizio SAP BTP – *SAP Business Technology Platform*.
- Manutenzione On Premise residua, post avvio della soluzione SAP CDC.

Per quanto riguarda il modello SAP CDC al termine della durata del contratto Sogei si riserva la possibilità di dare continuità all'attuale contratto in essere (parità di perimetro) o di definire un nuovo perimetro per SAP CDC. A parità di perimetro l'eventuale adeguamento dei prezzi dovrà essere limitato all'impatto dell'indice dei prezzi al consumo e non dovrà comunque eccedere il 3,3%.

In alternativa, Sogei avrà la possibilità di riattivare le licenze nel modello tradizionale e la relativa manutenzione, previa richiesta entro 30 giorni prima della scadenza del contratto (prevista 48 mesi successivi alla data di avvio della SAP CDC) e pagamento del corrispettivo del canone retroattivo di manutenzione a partire dalla data di avvio della SAP CDC.

4 CARATTERISTICHE DELLA FORNITURA

Nei seguenti paragrafi sarà fornito il dettaglio della soluzione e delle componenti che la costituiscono.

4.1 SAP CDC – Supporto operativo delle componenti legacy in fase di setup

In previsione della graduale transizione verso il nuovo modello SAP CDC, il software vendor SAP dovrà garantire la continuità operativa dei servizi erogati dal sistema legacy. In questa fase, il software vendor SAP dovrà garantire la piena operatività delle componenti legacy, assicurando la stabilità complessiva dell'ambiente durante il periodo di set-up. Tale supporto operativo dovrà essere fornito da SAP nella fase di setup.

La fase di setup, dunque la continuità operativa, dovrà essere prevista per le seguenti componenti:

- Servizio Cloud - *SAP Analytics Cloud (SAC)*;
- Servizio Cloud - *SAP Business Technology Platform (BTP)*;
- Servizio Manutenzione on premise.

Setup e continuità operativa Servizio Cloud SAP Analytics Cloud (SAC)

Di seguito si riporta l'elenco delle componenti afferenti alla soluzione *SAP Analytics Cloud (SAC)*, oggetto di setup operativo fino alla data di accensione di SAP CDC:

Prodotto	Metrica	Quantità
SAP Analyt Cloud, Plan Pred Prof Priv CF	1 Users	200
SAP Analyt Cloud, Plan Pred Std Priv CF	1 Users	4.800
SAP AnlCld HANA upd Pred Priv 512GB CF	256 GB of Memory	1
SAP AnlCld HANA upd Pred Priv 256GB CF	128 GB of Memory	1
SAP AnlCld HANA upd Pred Priv 1024GB CF	512 GB of Memory	1
SAP AnalytCloud test ten pred private CF	1 Users	50
SAP AnalytCloud test ten pred private CF	1 Users	50
SAP AnalytCloud test ten pred private CF	1 Users	50

Setup e continuità operativa Servizio Cloud SAP Business Technology Platform (BTP)

La piattaforma *SAP Business Technology Platform (BTP)*, utilizzata da Sogei per l'applicazione ReGis, consente alla Ragioneria Generale dello Stato di adempiere alle funzioni di gestione, monitoraggio, rendicontazione e controllo delle diverse componenti del PNRR. In particolare, lo strumento viene utilizzato come front-end da tutto il personale delle Amministrazioni centrali dello Stato e delle Amministrazioni autonome, consentendo alla

Ragioneria di disporre di una soluzione adattabile alle evoluzioni normative legate al PNRR e di raggiungere l'intero parco utenti delle applicazioni, favorendo la trasparenza amministrativa e la tempestiva comunicazione degli avanzamenti progettuali, sia a livello nazionale che europeo.

Di seguito si riporta l'elenco delle componenti afferenti alla soluzione SAP *Business Technology Platform* oggetto di setup operativo:

Prodotto	Metrica	Quantità per anno
Cloud Platform Ent Agrmt, reseller ed	Crediti cloud	1.700.000

Tali crediti cloud sono funzionali all'erogazione dei servizi SAP BTP necessari al funzionamento dell'applicazione ReGis e, più in generale, al supporto delle attività svolte dalla Ragioneria Generale dello Stato nell'ambito di ReGiS.

Il servizio di setup operativo della SAP *Business Technology Platform* dovrà prevedersi fino a data accensione della SAP CDC.

Setup e continuità operativa Servizio di Manutenzione on Premise

Di seguito si riporta l'elenco delle componenti per le quali il software vendor SAP dovrà garantire la continuità operativa del servizio nella fase preparatoria e di setup operativo per la SAP CDC.

Nel dettaglio, si riporta di seguito l'elenco delle applicazioni per le quali SAP dovrà garantire la continuità operativa del servizio di manutenzione:

- INIT-REGIS;
- SISTEMA FINANZIARIO IGRUE;
- BUSINESS OBJECT.

INIT-REGIS - Elenco delle componenti oggetto di setup operativo fino alla data di accensione di SAP CDC:

Prodotto	Quantità
Real Estate Portfolio and Workspace Management for SAP S/4HANA	1
S/4 Ent. Mgmt. Professional use	40000
S/4 Enterprise Mgmt. for Functional use	1
SAP Access Control for SAP S/4HANA	301
SAP Archiving by OpenText for SAP S/4HANA	30000
SAP Business Planning and Consolidation, version for Microsoft Platform, professional edition	15
SAP Business Planning and Consolidation, version for Microsoft Platform, standard edition	85
SAP Business Planning and Consolidation, version for SAP BW/4HANA (Standard)	100
SAP Business Planning and Consolidation, version for SAP BW/4HANA, Professional	3988

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

SAP BW/4HANA, up to 16 units	5
SAP Contract & Lease Mgmt for S/4HANA	1
SAP Disclosure Management, professional edition	5
SAP Disclosure Management, standard edition	1
SAP DP by OpenText for SAP S/4HANA	24
SAP DP by OpenText, add-on for BC S/4HANA	24
SAP Enable Now, author option	1
SAP Enable Now, consumption option	1
SAP Ent Proj Connect for SAP S/4HANA	1
SAP Inv Mgmt by OpenText for SAP S/4HANA	2000
SAP Landscape Management	4
SAP Process Control for SAP S/4HANA	450
SAP Process Orchestration	8
SAP Real Estate for S4, resid pr mgmt opt	1
SAP Real Estate Management for SAP S/4HANA, office, retail, and industrial property management option	1
SAP S/4HANA Finance, Cash Mang above 9000 units	9010
SAP S/4HANA Enterprise Portfolio and Project Management, professional	1
SAP S/4HANA Enterprise Portfolio and Project Management, standard	1
SAP S/4HANA, Developer access	80
SAP, EPPM professional	450
Tax, Benefits & Pay. Proc. for PS for S/4	3
Tax, Benefits & Paym. Proc. for PS for CRM	2
UI data protection logging for SAP S/4HANA	40
UI data protection masking for SAP S/4HANA	40

SISTEMA FINANZIARIO IGRUE - Elenco delle componenti oggetto di setup operativo fino alla data di accensione di SAP CDC:

Prodotto	Quantità
SAP Application Ltd. Prof. User	125
SAP Developer User	10
SAP ERP Foundation Starter	1
SAP NetWeaver Business Process Mgmt	5
SAP NetWeaver Business Rules Management	5
SAP NetWeaver Process Integration	5
SAP Professional User	5 (S/4 credit conversion)
SAP Professional User	245

BUSINESS OBJECT - Elenco delle componenti oggetto di setup operativo fino alla data di accensione di SAP CDC:

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

Prodotto	Metrica	Quantità	Iniziativa	Note
SAP BusinessObjects Enterprise (CS)	CS	33	Cross	Licenze necessarie per installazioni SAP BO non incluse nella SAP CDC (Progetto DAPA, CoGe e DAG)
SAP BusObj Enterprise Premium (CPU)	CPU	3	Cross	Licenze necessarie per installazioni SAP BO non incluse nella SAP CDC (Progetto DAPA e CoGe)
SAP BusObj Web Intelligence (CPU)	CPU	2	Cross	Licenze necessarie per installazioni SAP BO non incluse nella SAP CDC (Progetto DAPA e CoGe)

In riferimento alla licenza *SAP BusinessObjects Enterprise (CS)* si evidenzia che il prodotto include le seguenti funzionalità:

- *SAP BusinessObjects Business Intelligence platform,*
- *SAP BusinessObjects Mobile e SAP BusinessObjects Live Office*
- *SAP BusinessObjects Web Intelligence®*
- *SAP Analysis for Microsoft Office - SAP Lumira®, server edition*
- *SAP Crystal Reports® viewing*
- *SAP Analysis for OLAP Restricted-use runtime licenses*

4.2 SAP CDC – Diritto d'uso del Software

Di seguito si riporta l'elenco delle componenti software ad oggi in uso da Sogei che saranno ambito di evoluzione verso SAP CDC, considerando eventuali variazioni nei volumi legate ai nuovi fabbisogni.

Prodotto*	Metrica	Blocchi	Quantità Prevista in CDC
SAP Cloud ERP Private, tailored option	Full Use Equivalent	1	Fino a 60.000
SAP BW/4HANA, priv ed, tailored op	Tenant	1	2
SAP Business Planning and Consolidation professional edition for SAP BW/4HANA, priv ed, tailored op	User	1	6.700
SAP Business Planning and Consolidation standard edition for SAP BW/4HANA, priv ed, tailored op	User	1	100
SAP S/4HANA for Invoice Management by OpenText, priv ed, tailored op	Document	1000	2.000
SAP S/4HANA, Enterprise Portfolio and Project Management, priv ed, tailored op, professional	Active User	1	500
SAP Process Control, priv ed, tailored option	User	1	500
SAP S/4HANA for UI data protection logging, priv ed, tailored op	User	100	1.000

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

SAP S/4HANA for UI data protection masking, private edition, tailored option	User	100	1.000
SAP BusinessObjects Enterprise, private edition, tailored option (CS)	Connections	1	3.000
SAP BusinessObjects Business Intelligence, private cloud edition, tailored option, connection	Connections	1	7.000
SAP Process Orchestrator, private edition, tailored option	Cores	1	48
SAP S/4HANA, Digital Access, private edition, tailored option	Document	1000	100.000
SAP S/4HANA for Access Control, private edition, tailored option	Resources	100	5
SAP Solution Manager Enterprise Edition	Tenant	1	1
SAP AI Unit	Capacity Unit	100	1620 per anno

*La nomenclatura del prodotto potrà essere soggetta a cambiamenti da parte del software vendor.

Le licenze software comprese nel modello SAP CDC includono anche nuove esigenze progettuali di diverse iniziative Sogei relative ai prodotti SAP (es.: Ortes, ReGiS, BI su vari progetti, etc.).

Il servizio SAP CDC dovrà consentire l'abilitazione di scenari di intelligenza artificiale attraverso la componente SAP AI Unit.

Qualora, durante la durata contrattuale, a cause dell'evoluzione del modello SAP CDC, si rendano disponibili nuove licenze, funzionalità o *capabilities*, analoghe a quelle già incluse nel perimetro contrattuale, e tali elementi siano resi disponibili dal fornitore senza oneri aggiuntivi (a parità di condizioni economiche), la Committente potrà richiederne l'integrazione nel servizio fornito. Il Fornitore si impegna a includere tali elementi nel perimetro dell'offerta, senza variazioni di prezzo, previa richiesta formale della Committente.

In particolare, le componenti SW soggette ad incrementi relative a nuove progettualità sono:

- SAP Cloud ERP Private, tailored option, che introduce – come sopra riportato - una nuova metrica di distribuzione delle utenze: il *Full Usage Equivalent* (FUE). Il FUE può essere allocato, in piena autonomia da Sogei, secondo la seguente tabella di ponderazione, di seguito riportata:

FUE	USER	User Type
2	1	SAP S/4HANA Developer Access
1	1	SAP S/4HANA for advanced use
1	5	SAP S/4HANA for core use
1	30	SAP S/4HANA for self-service use

Saranno previsti un numero di 60.000 FUE che potranno consentire una allocazione ottimizzata delle utenze. A titolo esemplificativo e non esaustivo, ad esempio 10.000 FUE potranno essere allocati come segue:

- 50.000 utenti, SAP S/4HANA for Core Use;

- 10.000 utenti, SAP S/4HANA for Advanced Use;
- 300.000 utenti, SAP S/4HANA for Self-service Use.
- SAP BusinessObjects Business Intelligence, che, avendo un utilizzo pervasivo, prevede ad oggi un fabbisogno di sessioni concorrenti, stimato da Sogei sulla base delle attività di censimento, di 10.000 sessioni concorrenti, di cui 3.000 sessioni concorrenti che utilizzano le funzionalità della componente SAP Lumira (la metrica di riferimento è SAP BusinessObjects Enterprise, *priv ed, tailored option*) e le restanti 7.000 sessioni che utilizzano le funzionalità standard (metrica di riferimento SAP BusinessObjects Business Intelligence, *private cloud edition, tailored option, connection*). Nella soluzione SAP CDC si propone la seguente ripartizione delle sessioni concorrenti disponibili:

Censimento AS-IS			Proposta TO-BE	
Progetto	Utenti Nominali	Picco sessioni concorrenti	Sistema CDC	Allocazione Sessioni Concorrenti CDC
AreaRGS	27.038	19(*)	AreaRGS	3.000
BDAP	82.760	1.100	BDAP	2.000
DWRGS	2.264	700	DWRGS	1.000
IGRUE	2.536	375	REGIS	1.500
INIT/REGIS	3.302	53		1.500
Tessera Sanitaria	1.259	127	Tessera Sanitaria	150
			Buffer licenze CDC	850

* Area non ancora a regime, l'informazione sul picco è un dato non definitivo

La distribuzione descritta è indicativa e potrà essere rimodulata da Sogei in base alle effettive necessità di risorse.

- SAP Process Orchestrator, private edition, tailored option, per abilitare nuove esigenze di interoperabilità ed integrazione tra applicazioni ed in linea con il dimensionamento della SAP CDC;
- SAP S/4HANA, Enterprise Portfolio and Project Management, private edition, tailored option, professional, per abilitare fino a 500 utenti per le esigenze legate alla iniziativa ReGiS;
- SAP Process Control, private edition, tailored option, per abilitare fino a 500 utenti del sistema ReGiS per la creazione e gestione delle *check-list*;
- SAP S/4HANA, Digital Access, private edition, tailored option, per abilitare l'incremento di possibili accessi indiretti;

- SAP S/4HANA for Access Control, private edition, tailored option, per il controllo degli accessi relative alle attività di emergenza e relativa mitigazione dei rischi sulle utenze 'Firefighter'.

4.3 SAP CDC – Infrastruttura

Il modello SAP CDC include nella sottoscrizione il comodato d'uso dell'infrastrutture tecniche sottostanti le applicazioni software che saranno installate all'interno dei Data Center Sogei.

Anche nella componente HW, la SAP CDC si presenta come una soluzione ingegnerizzata e standardizzata da SAP come sistema completo, progettata con un alto grado di integrazione tra hardware, software e servizi, ottimizzata in fase di progettazione e di test, replicabile secondo standard predefiniti per garantire prestazioni elevate, affidabilità e semplicità di gestione.

Si riportano nel presente paragrafo le componenti logiche i sistemi in ambito e il relativo fabbisogno di risorse, dimensionato coerentemente ai principi di standardizzazione previsti da SAP CDC.

4.3.1 Architettura logica SAP CDC

L'architettura della SAP CDC è stata ingegnerizzata dal gruppo di ingegneria SAP congiuntamente con i responsabili dello sviluppo software SAP e l'ingegneria dei partner HW. Come illustrato nella figura seguente, lo standard architetturale definito per SAP CDC prevede che le componenti infrastrutturali siano ospitate sul sito primario, comprendente anche componenti di *business continuity*, e sul sito secondario (*Disaster Recovery*) di Sogei.

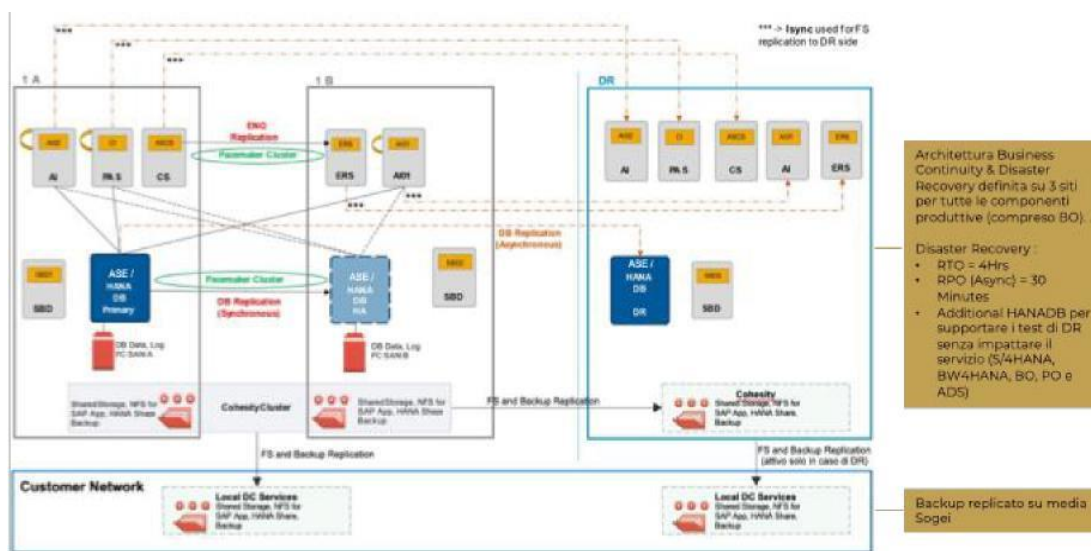


Figura 1 - Architettura SAP DC Primario (1A e 1B) e DC Secondario (DR)

Il sito primario, organizzato nella modalità Campus, ovvero con ridondanza HW su due siti (1A e 1B), garantirà attraverso il *cluster pacemaker* la continuità di servizio (*Business Continuity*).

Il sito secondario dovrà essere allineato attraverso meccanismi di replica, SAP HANA/ASE *system replication* per i database e *storage replication* per gli *application server*.

Per gli ambienti SAP S/4HANA, SAP BW/4HANA, SAP BO, SAP ADS e SAP PO dovranno essere disponibili istanze aggiuntive nel sito DR per poter effettuare test DR senza impattare la normale erogazione del servizio.

I meccanismi di *Business Continuity* e *Disaster Recovery* sono richiesti per i soli ambienti produttivi.

Il DR dovrà prevedere RTO=4h e RPO =30 min.

4.3.2 Architettura di integrazione di rete e SAN

Dal punto di vista di rete, SAP CDC si presenta come un'estensione della rete Sogei tramite la connessione di uplink ridondanti forniti da Sogei.

L'integrazione di rete avverrà a livello di rete L3 per cui non sono richiesti apparati specifici da parte di Sogei, a parte una corretta configurazione del *routing*.

A titolo esemplificativo, si riporta di seguito un possibile integrazione fisica tra la rete SAP CDC e la rete di un ipotetico cliente.

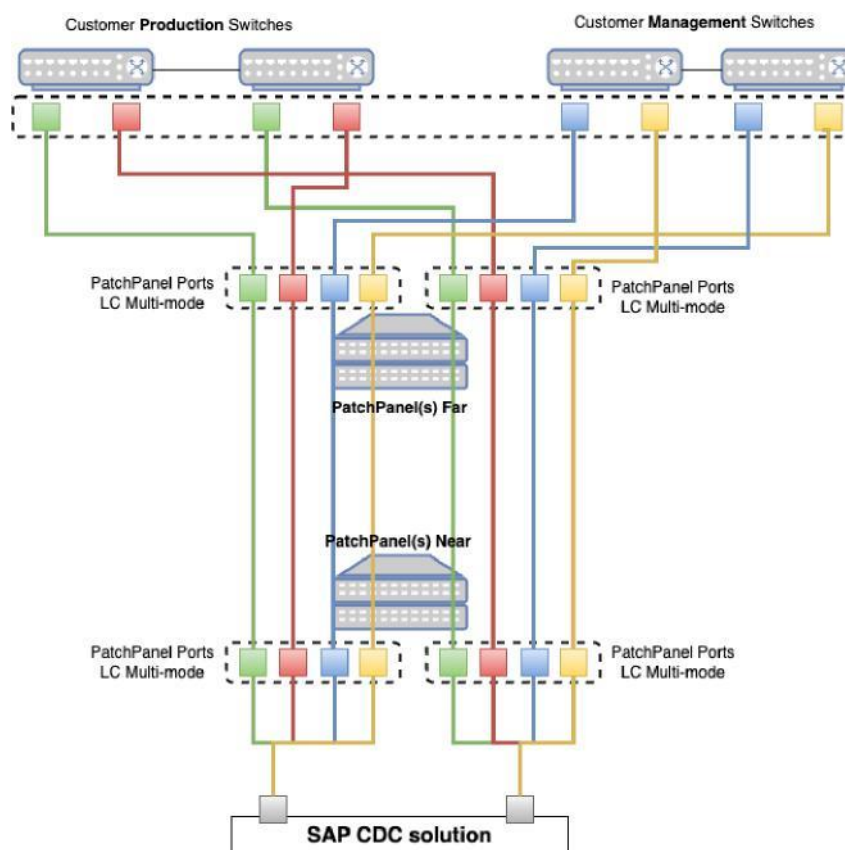


Figura 2 - possibile integrazione fisica tra la rete SAP CDC e la rete di un cliente

Sogei metterà a disposizione le *subnet* IP coerenti con il proprio contesto di rete, che verranno utilizzate per la configurazione di rete all'interno della SAP CDC. Questo renderà la rete logica all'interno della CDC un'estensione della rete Sogei.

A livello SAN e non è prevista alcuna integrazione con apparati esterni alla SAP CDC.

4.3.3 Piattaforme SAP in ambito

L'ambito delle piattaforme SAP che saranno ricondotte al modello SAP CDC è riportato nella seguente tabella.

N°	Piattaforma	Descrizione
1	S/4HANA INIT	Sistema ERP Core per la gestione dei processi in ambito INIT e ORTES (in fase progettuale)
2	S/4HANA ReGiS*	Sistema ERP Core per la gestione dei processi in ambito ReGiS
3	S/4HANA Play	Sistema ERP non produttivo per attività di sperimentazione utilizzabile da INIT e/o da ReGiS
4	SAP BW/4HANA INIT	Soluzione di backend a supporto della pianificazione e reporting per INIT

5	SAP BW/4HANA ReGiS	Soluzione di backend a supporto della pianificazione e reporting per ReGiS
6	SAP Process Orchestration	Componente tecnico di integrazione tra sistemi SAP e non SAP
7	SAP GRC	Soluzione di controllo processi in uso sui processi ReGiS
8	SAP Solution Manager 7.2	Componente tecnico per gestione del ciclo di vita del SW e monitoraggio sistemi SAP
9	SAP Adobe Document Services	Componente tecnico per visualizzazione PDF
10	SAP Business Objects INIT	Componente di Business Intelligence per il programma INIT
11	SAP Business Objects ReGiS	Componente di Business Intelligence per il programma ReGiS
12	SAP Business Objects AreaRGS	Componente di Business Intelligence per il programma AreaRGS
13	SAP Business Objects Tessera Sanitaria	Componente di Business Intelligence per il programma Tessera Sanitaria
14	SAP Business Objects DWHRGS	Componente di Business Intelligence per il programma DWHRGS
15	SAP Business Objects BDAP	Componente di Business Intelligence per il programma BDAP

**SAP S/4HANA – A tendere, è previsto che l'applicazione SAP IGRUE venga consolidata all'interno della piattaforma ReGiS. Il dimensionamento di quest'ultimo dovrà tenere presente delle risorse necessarie per il consolidamento delle due applicazioni.*

4.3.4 System Landscape / Sizing

La seguente tabella riporta la lista delle istanze applicative SAP con il relativo dimensionamento, basato su specifiche SAP CDC, e allocazione nei vari siti, che dovranno essere presi in considerazione per definire la configurazione della SAP CDC.

Applicazione	Sistema	SID	Ambiente	SITO 1A								SITO 1B								SITO DR							
				# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS
INIT	S/4HANA	S4P	Produzione	1	3904	192	6930	6	96	24	200	1	3904	192	6930	6	96	24	200	1	3904	192	6930	6	96	24	200
	S/4HANA	S4T	Test	1	960	64	6844	2	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	S4C	Collaudo	1	3904	192	6930	6	96	24	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	S4S	Sviluppo	1	384	32	1721	1	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	S2S	Sviluppo Parallelo	1	256	32	1247	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	S2C	Collaudo Parallelo	1	512	64	7033	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	S2T	Test Parallelo	1	256	32	6777	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	S2F	Formazione	1	3904	192	6930	4	64	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
Play INIT/ReGiS	S/4HANA	S4F	Play	1	256	32	6777	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--		
ReGiS	S/4HANA	R4P	Produzione	1	1984	120	4473	4	96	24	200	1	1984	120	4473	4	96	24	200	1	1984	120	4473	4	96	24	200
	S/4HANA	R4T	Test	1	960	64	4544	2	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	R4C	Collaudo	1	1984	120	4473	4	96	24	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	R4S	Sviluppo	1	256	32	1247	1	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	R2T	Test Parallelo	1	960	64	3244	2	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	

				SITO 1A								SITO 1B								SITO DR							
--	--	--	--	---------	--	--	--	--	--	--	--	---------	--	--	--	--	--	--	--	---------	--	--	--	--	--	--	--

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

Applicazione	Sistema	SID	Ambiente	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS
	S/4HANA	R2C	Collaudo Parallelo	1	1984	120	4473	2	96	24	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	S/4HANA	R2S	Sviluppo Parallelo	1	256	32	1247	1	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	S/4HANA	R4F	Formazione	1	1984	120	4473	2	96	24	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
BW/4 HANA Init	BW/4HANA	BPS	Sviluppo	1	256	32	1247	1	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	BPT	Test	1	256	32	1247	1	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	BPC	Collaudo	1	1472	64	3858	4	64	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	BPP	Produzione	1	1472	64	3858	4	64	12	200	1	1472	64	3858	4	64	12	200	1	1472	64	3858	4	64	12	200
	BW/4HANA	B2S	Sviluppo Parallelo	1	256	32	1247	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	B2T	Test Parallelo	1	256	32	1247	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	B2C	Collaudo Parallelo	1	512	64	4114	2	64	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	B2F	Formazione	1	512	64	4114	2	64	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	B2G	Test Parallelo	1	256	32	1247	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
BW/4HANA ReGiS	BW/4HANA	BRS	Sviluppo	1	256	32	1247	1	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	BRT	Test	1	256	32	1247	1	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	BRC	Collaudo	1	1984	120	4473	4	64	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	BW/4HANA	BRP	Produzione	1	1984	120	4473	4	64	12	200	1	1984	120	4473	4	64	12	200	1	1984	120	4473	4	64	12	200
PO	PO	POS	Sviluppo	1	128	32	774	1	24	8	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	PO	POT	Test	1	128	32	774	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	PO	POC	Collaudo	1	256	32	1247	4	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	
	PO	POP	Produzione	1	256	32	1247	4	48	12	200	1	256	32	1247	4	48	12	200	1	256	32	1247	4	48	12	200
GRC	GRC Process	GRS	Sviluppo	1	256	32	1247	1	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

Applicazione	Sistema	SID	Ambiente	SITO 1A								SITO 1B								SITO DR							
				# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS
	GRC Process	GRC	Collaudo	1	256	32	1247	2	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	GRC Process	GRP	Produzione	1	256	32	1247	2	32	12	200	1	256	32	1247	2	32	12	200	1	256	32	1247	2	32	12	200
ADS	Adobe Document Services	ADS	Sviluppo	1	128	32	774	1	16	8	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Adobe Document Services	ADT	Test	1	128	32	774	2	24	8	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Adobe Document Services	ADC	Collaudo	1	128	32	774	2	48	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Adobe Document Services	ADP	Produzione	1	128	32	774	2	48	12	200	1	128	32	774	2	48	12	200	1	128	32	774	2	48	12	200
SolMan	Solution Manager	SMS	Sviluppo	1	256	32	1247	2	32	12	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Solution Manager	SMP	Produzione	1	256	32	1247	2	96	12	200	1	256	32	1247	2	96	12	200	1	256	32	1247	2	96	12	200
Web Dispatcher	WD Interno	--	Sviluppo	--	--	--	--	1	24	8	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	WD Interno	--	Test	--	--	--	--	2	24	8	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	WD Interno	--	Collaudo	--	--	--	--	2	96	24	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	WD Esterno	--	Collaudo	--	--	--	--	2	96	24	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	WD M2M	--	Collaudo	--	--	--	--	2	96	24	200	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	WD Interno	--	Produzione	--	--	--	--	2	96	24	200	--	--	--	--	2	96	24	200	--	--	--	--	2	96	24	200
	WD Esterno	--	Produzione	--	--	--	--	2	96	24	200	--	--	--	--	2	96	24	200	--	--	--	--	2	96	24	200
	WD M2M	--	Produzione	--	--	--	--	2	96	24	200	--	--	--	--	2	96	24	200	--	--	--	--	2	96	24	200
Sandbox DR S/4HANA Init	S/4HANA	--	Sandbox DR	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	3904	--	--	Riutilizzo temporaneo AS presenti in DR			
Sandbox DR S/4HANA Regis	S/4HANA	--	Sandbox DR	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1984	--	--	Riutilizzo temporaneo AS presenti in DR			

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

Applicazione	Sistema	SID	Ambiente	SITO 1A								SITO 1B								SITO DR							
				# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS	# DB Server	Dimensione DB (GB)	CPU DB (GB)	Storage DB	#App servers	App Server RAM (GB)	App Server vCPU	Storage per singolo AS
Sandbox DR BW/4HANA Init	BW/4HANA	--	Sandbox DR	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1472	--	--	Riutilizzo temporaneo AS presenti in DR			
Sandbox DR BW/4HANA Regis	S/4HANA	--	Sandbox DR	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1984	--	--	Riutilizzo temporaneo AS presenti in DR			
Sandbox DR SAP ADS	S/4HANA	--	Sandbox DR	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	128	--	--	Riutilizzo temporaneo AS presenti in DR			
Sandbox DR SAP PO	BW/4HANA	--	Sandbox DR	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	256	--	--	Riutilizzo temporaneo AS presenti in DR			
Agent SDI	Agent SDI	--	Sviluppo	--	--	--	--	1	32	12	50	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Agent SDI	--	Sviluppo/Test	--	--	--	--	2	32	12	50	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
	Agent SDI	--	Produzione	--	--	--	--	2	32	12	50	--	--	--	--	2	32	12	50	--	--	--	--	2	32	12	50

Si precisa inoltre che i sistemi SAP S4T, S2C, S2T, S4F, R4T, B2C e B2F sono stati dimensionati, in termini di storage DB, per consentire di effettuare attività di ribaltamento dati dall'ambiente produttivo.

All'interno della SAP CDC sono previste come da standard anche le componenti SAP Router e SAP Cloud Connector. Sogei potrà valutare l'utilizzo di queste componenti all'interno della SAP CDC oppure mantenere quelle in essere nella modalità OnPremise.

La seguente tabella riporta la lista delle istanze applicative SAP BusinessObject con il relativo dimensionamento, basato su specifiche SAP CDC, e allocazione nei vari siti, che dovranno essere presi in considerazione per definire la configurazione della SAP CDC.

Applicazione	Ambiente	Componente	SITO 1A				SITO 1B				SITO DR			
			# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# DB Server	# VM Server	CPU VM	RAM VM (GB)
INIT	Sviluppo	Tomcat WS + WAS BO	1	12	64	200	--	--	--	--	--	--	--	--
	Sviluppo	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Test	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Test	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Test	WAS BO	1	8	16	100	--	--	--	--	--	--	--	--
	Test	WAS BO	1	8	16	100	--	--	--	--	--	--	--	--
	Test	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Test	FSR (File System Repository)	0	--	--	100	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Collaudo	WAS BO	1	12	64	100	--	--	--	--	--	--	--	--
	Collaudo	WAS BO	1	12	64	100	--	--	--	--	--	--	--	--
	Collaudo	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Collaudo	FSR (File System Repository)	0	--	--	200	--	--	--	--	--	--	--	--
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50

Applicazione	Ambiente	Componente	SITO 1A				SITO 1B				SITO DR			
			# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# DB Server	# VM Server	CPU VM	RAM VM (GB)
	Produzione	WAS BO	1	12	64	100	1	12	64	100	1	12	64	100
	Produzione	WAS BO	1	12	64	100	1	12	64	100	1	12	64	100
	Produzione	Database (CMS Server)	1	12	32	1133	1	12	32	1133	1	12	32	1133
	Produzione	FSR (File System Repository)	0	--	--	200	0	--	--	200	0	--	--	200
	Pre-Produzione	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Pre-Produzione	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Pre-Produzione	WAS BO	1	12	64	100	--	--	--	--	--	--	--	--
	Pre-Produzione	WAS BO	1	12	64	100	--	--	--	--	--	--	--	--
	Pre-Produzione	Database (CMS Server)	1	12	32	668	--	--	--	--	--	--	--	--
	Pre-Produzione	FSR (File System Repository)	0	--	--	300	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Tomcat WS + WAS BO	1	12	64	100	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
AreaRGS	Sviluppo	Tomcat WS + WAS BO	1	12	64	200	--	--	--	--	--	--	--	--
	Sviluppo	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Tomcat WS + WAS BO	1	12	64	500	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Pre-Produzione	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Pre-Produzione	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Pre-Produzione	WAS BO	1	24	96	100	--	--	--	--	--	--	--	--

Applicazione	Ambiente	Componente	SITO 1A				SITO 1B				SITO DR			
			# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# DB Server	# VM Server	CPU VM	RAM VM (GB)
	Pre-Produzione	WAS BO	1	24	96	100	--	--	--	--	--	--	--	--
	Pre-Produzione	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Pre-Produzione	FSR (File System Repository)	0	--	--	300	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Collaudo	WAS BO	1	24	96	100	--	--	--	--	--	--	--	--
	Collaudo	WAS BO	1	24	96	100	--	--	--	--	--	--	--	--
	Collaudo	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Collaudo	FSR (File System Repository)	0	--	--	300	--	--	--	--	--	--	--	--
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50
	Produzione	WAS BO	1	24	96	100	1	24	96	100	1	24	96	100
	Produzione	WAS BO	1	24	96	100	1	24	96	100	1	24	96	100
	Produzione	WAS BO	1	24	96	100	1	24	96	100	1	24	96	100
	Produzione	WAS BO	1	24	96	100	1	24	96	100	1	24	96	100
	Produzione	Database (CMS Server)	1	12	32	1133	1	12	32	1133	1	12	32	1133
	Produzione	FSR (File System Repository)	0	--	--	500	0	--	--	500	0	--	--	500

Applicazione	Ambiente	Componente	SITO 1A				SITO 1B				SITO DR			
			# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# DB Server	# VM Server	CPU VM	RAM VM (GB)
ReGIS	Sviluppo	Tomcat WS + WAS BO	1	12	64	200	--	--	--	--	--	--	--	--
	Sviluppo	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Test	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Test	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Test	WAS BO	1	8	16	100	--	--	--	--	--	--	--	--
	Test	WAS BO	1	8	16	100	--	--	--	--	--	--	--	--
	Test	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Test	FSR (File System Repository)	0	--	--	100	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS	1	8	16	50	--	--	--	--	--	--	--	--
	Collaudo	WAS BO	1	12	64	100	--	--	--	--	--	--	--	--
	Collaudo	WAS BO	1	12	64	100	--	--	--	--	--	--	--	--
	Collaudo	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Collaudo	FSR (File System Repository)	0	--	--	200	--	--	--	--	--	--	--	--
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50
	Produzione	Tomcat WS	1	8	16	50	1	8	16	50	1	8	16	50
	Produzione	WAS BO	1	12	64	100	1	12	64	100	1	12	64	100
	Produzione	WAS BO	1	12	64	100	1	12	64	100	1	12	64	100
	Produzione	Database (CMS Server)	1	12	32	1133	1	12	32	1133	1	12	32	1133

		Componente	SITO 1A	SITO 1B	SITO DR
--	--	------------	---------	---------	---------

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

Applicazione	Ambiente		# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# DB Server	# VM Server	CPU VM	RAM VM (GB)
	Produzione	FSR (File System Repository)	0	--	--	200	0	--	--	200	0	--	--	200
Tessera sanitaria BO TS*	Sviluppo	Tomcat WS + AS BO	1	12	32	200	--	--	--	--	--	--	--	--
	Sviluppo	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Validazione	Tomcat WS	1	4	8	60	--	--	--	--	--	--	--	--
	Validazione	Tomcat WS	1	4	8	60	--	--	--	--	--	--	--	--
	Validazione	AS BO	1	8	16	100	--	--	--	--	--	--	--	--
	Validazione	AS BO	1	8	16	100	--	--	--	--	--	--	--	--
	Validazione	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Validazione	FSR (File System Repository)	0	--	--	200	--	--	--	--	--	--	--	--
	Produzione	Tomcat WS	1	4	8	60	1	4	8	60	1	4	8	60
	Produzione	Tomcat WS	1	4	8	60	1	4	8	60	1	4	8	60
	Produzione	AS BO	1	12	32	150	1	12	32	150	1	12	32	150
	Produzione	AS BO	1	12	32	150	1	12	32	150	1	12	32	150
	Produzione	Database (CMS Server)	1	12	32	1133	1	12	32	1133	1	12	32	1133
	Produzione	FSR (File System Repository)	0	--	--	300	0	--	--	300	0	--	--	300
DWHRS	Sviluppo	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Sviluppo	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--

* Tessera Sanitaria in SAP CDC utilizzerà la componente Tomcat Web Services invece di Websphere.

Applicazione	Ambiente	Componente	SITO 1A				SITO 1B				SITO DR			
			# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# DB Server	# VM Server	CPU VM	RAM VM (GB)
	Collaudo	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Collaudo	FSR (File System Repository)	0	--	--	50	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Pre-Produzione	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Pre-Produzione	Database (CMS Server)	1	12	32	668	--	--	--	--	--	--	--	--
	Produzione	WAS BO	1	24	96	100	1	24	96	100	1	24	96	100
	Produzione	WAS BO	1	24	96	100	1	24	96	100	1	24	96	100
	Produzione	Lumira**	1	12	64	80	1	12	64	80	1	12	64	80
	Produzione	Lumira**	1	12	64	80	1	12	64	80	1	12	64	80
	Produzione	Database (CMS Server)	1	12	32	1133	1	12	32	1133	1	12	32	1133
	Produzione	FSR (File System Repository)	0	--	--	300	0	--	--	300	0	--	--	300
	Produzione	Tomcat WS	1	8	24	50	1	8	24	50	1	8	24	50
	Produzione	Tomcat WS	1	8	24	50	1	8	24	50	1	8	24	50
BDAP	Produzione	Tomcat WS	1	8	24	50	1	8	24	50	1	8	24	50
	Produzione	Tomcat WS	1	8	24	50	1	8	24	50	1	8	24	50
	Produzione	WAS BO	1	24	96	120	1	24	96	120	1	24	96	120
	Produzione	WAS BO	1	24	96	120	1	24	96	120	1	24	96	120
	Produzione	Lumira**	1	12	64	80	1	12	64	80	1	12	64	80

** La versione SAP Lumira prevista in SAP CDC è SAP LUMIRA SERVER FOR BIPLATFORM

		Componente	SITO 1A	SITO 1B	SITO DR
--	--	------------	---------	---------	---------

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

Applicazione	Ambiente		# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# VM Server	CPU VM	RAM VM (GB)	Storage VM (GB)	# DB Server	# VM Server	CPU VM	RAM VM (GB)
	Produzione	Lumira**	1	12	64	80	1	12	64	80	1	12	64	80
	Produzione	Database (CMS Server)	1	12	32	1133	1	12	32	1133	1	12	32	1133
	Produzione	FSR (File System Repository)	0	--	--	200	0	--	--	200	0	--	--	200
	Sviluppo	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Sviluppo	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Collaudo	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Collaudo	Database (CMS Server)	1	12	32	420	--	--	--	--	--	--	--	--
	Collaudo	FSR (File System Repository)	0	--	--	50	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Manutenzione / Correttiva	Database (CMS Server)	1	12	32	395	--	--	--	--	--	--	--	--
	Pre-Produzione	Tomcat WS + WAS BO	1	12	32	100	--	--	--	--	--	--	--	--
	Pre-Produzione	Database (CMS Server)	1	12	32	668	--	--	--	--	--	--	--	--
BDAP	Produzione	Database (CMS Server)	--	--	--	--	--	--	--	--	1	12	32	930

La configurazione della SAP CDC dovrà prevedere la possibilità di scalare sulla base delle evoluzioni dei requisiti applicativi supportando i seguenti scenari:

- Scalabilità verticale: dovrà prevedersi la possibilità di incrementare le risorse assegnate ai sistemi esistenti aggiornandone la configurazione virtuale;
- Scalabilità orizzontale: nel caso in cui venga raggiunto il limite di scalabilità verticale del singolo sistema, la soluzione applicativa dovrà prevedere la possibilità di scalare in modalità orizzontale, aggiungendo ulteriori sistemi a quelli già operativi;
- Scalabilità funzionale: dovrà essere possibile estendere le soluzioni contrattualizzate con nuovi *engine*/applicazioni per soddisfare nuovi requisiti.

Inoltre, vista la criticità dei servizi erogati da Sogei, è stata prevista capacità aggiuntiva non attiva e non compresa nel perimetro dell'acquisizione, che potrà essere utilizzata esclusivamente per far fronte ad eventuali esigenze future di ampliamento/scalabilità della soluzione SAP CDC.

4.4 SAP CDC – Servizi

4.4.1 Servizi di gestione della SAP CDC

Il modello SAP CDC in qualità di servizio gestito, oltre ad includere il diritto d'uso di software ed infrastruttura in comodato d'uso, prevede l'erogazione dei servizi tecnici di gestione, forniti dal *software vendor* SAP.

Nel modello SAP CDC la governance ed il coordinamento delle *operations* sono in carico a Sogei mentre le attività operative (*Technical Managed Service*) sono eseguite da SAP tramite il team operativo SAP ECS. Si riporta di seguito una rappresentazione complessiva del modello di gestione ed evoluzione delle piattaforme SAP con focus sui ruoli e macro-attività sottostante al modello SAP CDC.

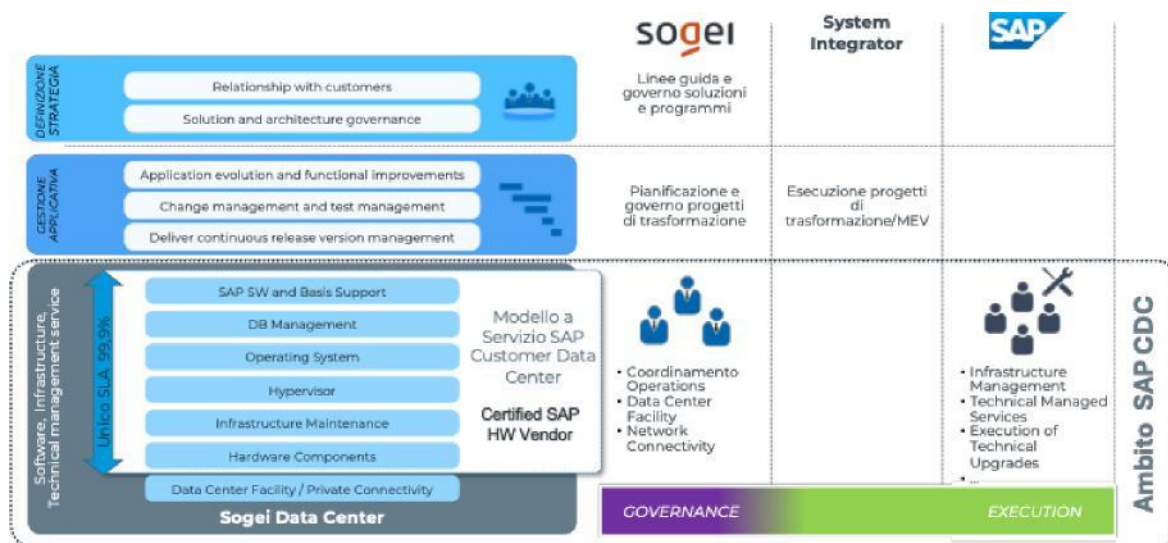


Figura 3 – Rappresentazione ruoli e macroattività

Il modello SAP CDC prevede una demarcazione delle attività in carico a SAP e di quelle in carico a SOGEI. La figura seguente riassume per macroaree la responsabilità sulle componenti di gestione.

		Componenti	SAP CDC
Gestione dei Processi di Business	Contesto Business	Innovazione continua con i rilasci delle applicazioni	SOGEI
		Correzione dell'interruzione dell'applicazione e supporto dell'applicazione funzionale	SOGEI
Gestione Applicativa Funzionale	Applicativo	Gestione del cambiamento, gestione dei rilasci e del deployment	SOGEI
	Middleware / Piattaforma	Configurazione dell'applicazione, Test ed Execution Management	SOGEI
Gestione Tecnica del Landscape	Middleware / Piattaforma	SLA per il tempo di attività dell'applicazione. Risorse denominate per il supporto operativo e la pianificazione dell'Engagement	SAP
	Database	Servizio di Disaster Recovery, Backups, monitoring, capacity reporting, Dashboard	SAP
	Sistema Operativo	Applicazione tecnica di aggiornamenti/upgrade per sistemi gestiti (pacchetti di supporto, patch, aggiornamenti e upgrade delle revisioni HANA, ecc.)	SAP
Gestione Infrastrutturale	Compute, Storage, e Virtualizzazione	Configurazione, creazione di sistemi e distribuzione di applicazioni basate sull'architettura di riferimento SAP CDC	SAP
	Gestione Infrastrutturale	Sistema Operativo, configurazione Database e Gestione	SAP
	Data Center Facility	Piattaforma dell'infrastruttura e gestione dell'interfaccia	SAP w/ HW Vendor
		Fornitura hardware / servizi di installazione e manutenzione	SAP w/ HW Vendor
		Sicurezza fisica e networking fino al primo rack	SOGEI
		Data center, alimentazione, raffreddamento e spazio fisico	SOGEI

Figura 4 - Responsabilità conduzione SAP CDC

Si riporta di seguito l'elenco dei servizi, forniti dal *software vendor* SAP secondo le modalità previste dal Codice, inclusi nel modello standard SAP CDC nonché l'elenco di ulteriori servizi necessari per rispondere ad esigenze specifiche Sogei di operations e progettuali:

- SAP Technical Managed Services, servizi inclusi nel modello standard SAP CDC;
- SAP Enhanced Operations Services, servizi che permettono di incrementare i livelli di servizio previsti dal modello standard SAP CDC;

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

- Servizi Tecnico Applicativi Aggiuntivi (rispetto a quelli inclusi nel modello standard), servizi a supporto delle operations Sogei;
- Servizi Addizionali (rispetto a quelli inclusi nel modello standard), servizi a copertura di eventuali richieste al momento non pianificate.

Il nuovo modello SAP CDC, comprensivo dei servizi sopra citati, prevederà il coinvolgimento di un team dedicato per Sogei caratterizzato dalle seguenti figure chiave: *Customer Delivery Manager, Technical Service Manager, SAP Architect, Database Engineer, Infrastructure Engineer*.

Il team opererà sotto la governance ed il coordinamento della struttura ingegneria, infrastrutture e data center di Sogei e supporterà il cliente nell'adozione di metodologie, strumenti e conduzione di task volti ad ottimizzare la *system administration* e più in generale le attività di *operations*.

In caso di necessità di supporto, Sogei potrà avvalersi, oltre al team dedicato, anche della piattaforma di *ticketing* SAP per l'apertura delle *service request* e di eventuali segnalazioni; la piattaforma dovrà prevedere un supporto 24*7 sia su sistemi produttivi che non.

Lo strumento di *ticketing* dovrà consentire una tracciatura puntuale dell'avanzamento della *service request*, con evidenza delle tempistiche di presa in carico e di processamento della richiesta data la complessità dell'attività richiesta.

Il supporto operativo di secondo e terzo livello nella risoluzione delle problematiche (es. *Troubleshooting*) rispetta i seguenti livelli di servizio.

Priorità	Tempo di reazione all'incidente (IRT)	SLA per IRT
1 – Molto Alta	Il tempo di reazione parte da quando il Livello 1 di Supporto SAP è contattato per l'incidente e la prima azione è intrapresa dalla persona del support SAP per la risoluzione dello stesso.	20 minuti (7*24h) (piano di risoluzione del problema entro 4 ore)
2 – Alta		2 ore
3 – Medio		4 ore
4 – Bassa		1 Giorno Lavorativo

L'ingegneria di SAP sarà responsabile e avrà il controllo delle attività sull'infrastruttura dedicata unicamente a SAP CDC, avvalendosi dell'eventuale coinvolgimento diretto del HW vendor e/o delle strutture competenti Sogei. Sogei dovrà avere l'opzione di rimuovere tale vincolo qualora decidesse di attivare la procedura di *Service Continuity Plan* (vedi Allegato 1).

4.4.1.1 SAP Technical Managed Services

Il modello SAP CDC prevede l'erogazione dei servizi tecnici di gestione da remoto sotto il governo e la guida di Sogei. Si riportano di seguito, a titolo esemplificativo e non esaustivo, le principali aree di intervento del SAP TMS.

- *Infrastructure management & Technical Managed Services*
 - Setup, *deploy* e manutenzione dell'infrastruttura
 - Gestione della rete e dello storage
 - Backup standard e *retention*
- *Managed Service*
 - Gestione ed esercizio di sistemi operativi e database (OS/DB)
 - Architettura e *deploy* secondo le best practice
 - Supporto tecnico di base e operativo
 - *SAP secure framework* e reporting di compliance
 - Reportistica e allineamento regolare con il team *Customer Delivery Engagement*
- *Execution of Technical Upgrade*
 - Modifiche tecniche (parametri, copie client, ecc.)
 - Applicazione di patch/aggiornamenti
 - Esecuzione tecnica dei pacchetti di supporto e degli aggiornamenti di versione

Si rimanda alla matrice Ruoli e Responsabilità per l'elenco di dettaglio (https://www.sap.com/about/agreements/policies/hec-services.html?sort=latest_desc&tag=language%3Aenglish&tag=agreements%3Aproduct-policy%2Fecs%2Froles-and-responsibilities&pdf-asset=3e742235-cc7e-0010-bca6-c68f7e60039b&page=1).

4.4.1.2 SAP Enhanced Operations Services

Con l'obiettivo di rafforzare e ottimizzare il modello SAP CDC saranno da includersi i servizi *SAP Enhanced Operations Services* (EOS) che, sotto il coordinamento e la governance delle strutture *Operations/Architettura Sogei*, permetteranno di incrementare i livelli di servizio previsti dal modello standard.

Si riporta di seguito una tabella sinottica che sintetizza le aree di miglioramento apportate dai servizi *Enhanced Operations Services* rispetto allo standard di servizio SAP CDC.

Area	Descrizione	Servizio Standard SAP CDC	Enhanced Operational Service SAP CDC per Sogei
------	-------------	---------------------------	--

ECS Core Team	L'erogazione ECS è composta dai seguenti ruoli: <i>Customer Delivery Manager;</i> <i>Technical Service Manager;</i> <i>SAP Architect;</i> <i>Database Engineer;</i> <i>Infrastructure Engineer.</i>	<i>Customer Delivery Manager</i> (nominato); <i>Technical Service Manager</i> (nominato)	<i>Customer Delivery Manager</i> (dedicato); <i>Technical Service Manager</i> (dedicato); <i>SAP Architect</i> (nominato); <i>Database Engineer</i> (nominato); <i>Infrastructure Engineer</i> (nominato)
Service Level Agreement per sistemi non produttivi (SLA)	Disponibilità del sistema per ambienti non produttivi Orari <i>Service Request</i> per ambienti non produttivi	Disponibilità sistema: SLA 95%, Orari <i>Service Request</i> : SLA 24h x 5 giorni	Disponibilità sistema: SLA 98%, Orari <i>Service Request</i> : SLA 24h x 7 giorni
EU Access	SAP e/o sub-responsabili situati nello Spazio Economico Europeo (SEE) o Svizzera (CH) elaborano dati personali secondo l'EU Access	Non incluso	Dipendenti SAP o dei sub-responsabili che supportano il cliente si trovano in un paese approvato per l'EU Access
Servizi di Business Continuity	Strumenti e metodi avanzati per implementare aggiornamenti sulla soluzione SAP gestita, minimizzando i tempi di inattività	Non incluso	Incluso nell'EOS, aiuta a ridurre i <i>downtime</i> durante le operazioni e la manutenzione dei servizi gestiti tecnici
LogServ	Servizio ECS per archiviare e accedere ai log generati dal cloud privato, migliorando la sicurezza. Permette di raccogliere e centralizzare i log di tutti i sistemi e applicazioni in uso	Non incluso	Raccolta log quasi in tempo reale Possibilità di integrazione con SIEM o sistema di gestione log Politica di conservazione standard 1 anno (estendibile fino a 10 anni con costi aggiuntivi) Recupero log conservati da ECS
Hypercare	Salvaguardia delle fasi critiche del ciclo di vita della soluzione SAP ECS. <i>Hypercare</i> offre servizi e controlli intensivi durante periodi di progetto critici come <i>GoLive</i> , <i>Business Cutover</i> , Migrazioni, ecc..	Non incluso	Incluso nell'EOS e si riferisce a SAP <i>NetWeaver</i> , Database (SAP <i>HANA</i> , SAP <i>ASE</i>) e sistema operativo e infrastruttura sottostanti


Servizio di Benchmarking delle Prestazioni	Focus sulle transazioni business più critiche del sistema ERP centrale del cliente	Non incluso	<p>Deliverable:</p> <p>Misurazione iniziale e trimestrale delle transazioni selezionate</p> <p>report trimestrale sui risultati</p> <p>valutazione congiunta dei risultati</p> <p>analisi delle <i>root cause</i> in caso di deviazioni per il solo <i>stack</i> tecnico</p> <p>Il servizio è fornito fino a 3 sistemi produttivi</p>
Framework Avanzato	<p>Set aggiuntivo di KPI di servizio combinati in un Service Quality Framework. Questi KPI saranno inclusi nel report mensile e saranno oggetto di revisione all'interno delle regolari riunioni di revisione del servizio tra il cliente e SAP.</p> <p>KPI:</p> <p>Tempo di consegna delle <i>Root Cause Analysis</i></p> <p>Tempo di risoluzione degli incidenti</p> <p>Comunicazione iniziale al cliente</p> <p>Conformità alle patch di sicurezza online del sistema operativo</p> <p>Rispetto della pianificazione</p> <p>Correttezza al primo tentativo</p> <p>Disponibilità del sistema su tutto il <i>landscape</i></p> <p>Rispetto del piano e della pianificazione</p> <p>Tasso di successo delle modifiche</p>	Non offerto	<p>Se uno o più KPI non sono rispettati, il cliente può notificare il responsabile SAP assegnato e richiedere un'analisi dei KPI.</p> <p>SAP procederà quindi tempestivamente a:</p> <ul style="list-style-type: none"> - Determinare <i>root cause</i> o la possibile <i>root cause</i> del mancato rispetto del KPI (se nota); e, salvo che il mancato rispetto sia giustificato, - Sviluppare un piano di azione correttiva e sottoporre tale piano al Cliente per approvazione scritta (che non sarà irragionevolmente negata o ritardata); e - Implementare il piano entro un periodo ragionevole (e in conformità con le tempistiche concordate).

4.4.1.3 Servizi tecnico/applicativi aggiuntivi

Con l'obiettivo di supportare ulteriormente le *operations* relative al modello di servizio SAP CDC, dovranno essere inclusi i servizi tecnico-applicativi aggiuntivi che andranno a fornire:

- Supporto operativo di secondo livello nella gestione ordinaria dei sistemi e risoluzione delle problematiche (es. *Troubleshooting*, *ABAP dump*, etc)
- Monitoraggio applicativo dei processi critici
- Supporto alle procedure di testing basato sull'automazione e sulla *change impact analysis*

Servizi inclusi	Servizi aggiuntivi		Servizi Applicativi
Standard	Optional	Additional	Application
Infrastructure Management & Technical Managed Services <ul style="list-style-type: none"> Infrastructure setup, deployment, and maintenance Network and storage management Standard backup and retention 	Disaster Recovery <ul style="list-style-type: none"> Implement disaster recovery setup Develop and use disaster recovery procedures for database and file system replication Ongoing management of disaster recovery architecture/monitoring Execute failover during disaster recovery test (DB, application, and names) Execute production failover in case of an officially declared disaster by provider 	Application Operations Customer Application Monitoring Regression Testing Performance Testing Deployment Management Application Security Updates Operation Improvement	
Managed Service <ul style="list-style-type: none"> OS, DB management and operations Best practice architecture and deployment Technical Basis and operations support SAP security framework and compliance reporting 24x7 monitoring and operational support Regular cadence and reporting with Customer Delivery Engagement team 	Infrastructure / DB extension (*) <ul style="list-style-type: none"> Scale compute capacity (memory and CPU) Scale storage capacity Add/remove HANA node to adjust SAP HANA capacity (N/A) Creation of additional tenants (N/A) Install HANA cockpit on new HANA database or tenant Increase system capacity by adding components 		
Execution of Technical Upgrades <ul style="list-style-type: none"> Technical changes (parameters, client copies, system copies, ...) Patching/updating Technical execution of support packages and version upgrades 	Other One-off tasks (*) <ul style="list-style-type: none"> Partition tables (technical execution) Setup and operated encrypted database post implementation System rebuild Separate domain migration ... 		



◆ ——— Attività eseguite da SAP ——— ◆

◆ ——— Attività eseguite dal Cliente/ System Integrator / SAP ——— ◆

Nell'approfondimento del modello SAP CDC sono stati integrati il servizio di Disaster Recovery (servizio opzionale) e alcuni servizi operativi relativi all'area applicativa (Application Service).

I servizi applicativi identificati con Sogei potranno essere rimodulati in modo flessibile per rispondere a eventuali variazioni delle esigenze.

Figura 5 - Potenziamento dei servizi standard SAP CDC

Servizi Tecnico/Applicativi Aggiuntivi	Package Code	Metrica di Utilizzo (per anno)
Security Updates	S1	4 sistemi produttivi (2 S/4HANA, BW/4HANA, PO)

Monitoraggio Applicativo	M2	<p>Monitoraggio SAP Managed FRUN da EU (10*5)</p> <ul style="list-style-type: none"> Fino a 5 sistemi di produzione (2 S/4 HANA, BW, PO e Solman ABAP) Fino a 150 interfacce PO Fino a 30 interfacce non PO <ul style="list-style-type: none"> Fino a 5 Idocs Fino a 5 RFC Fino a 20 Webservices ABAP <p>Creazione dei ticket: ~ fino a 40 al mese</p> <ul style="list-style-type: none"> Apertura di <i>incident</i> (per conto del cliente) basati sul monitoraggio applicativo tramite alert verso il team infrastruttura ECS per problematiche infrastrutturali. Una volta aperto il ticket infrastrutturale, la responsabilità (chiusura del ticket, aggiornamento dello stato nello strumento e reportistica mensile) sarà del team infrastruttura ECS. <p>Fino a 80 attività di remediation al mese tra le seguenti</p> <table border="1"> <thead> <tr> <th>#</th><th>Descrizione Alert</th><th>Attività di Remediation</th></tr> </thead> <tbody> <tr> <td>1</td><td>Carico utente elevato su sistema o istanza ABAP</td><td>Terminazione dell'attività utente relativa a <i>statement</i> costosi identificati</td></tr> <tr> <td>2</td><td>Elaborazione <i>Enqueue</i></td><td>Cancellazione dei <i>lock Enqueue</i></td></tr> <tr> <td>3</td><td>Uso elevato della memoria ABAP</td><td>Modifica temporanea dell'allocazione <i>heap</i> o memoria estesa tramite <i>RSMEMORY</i></td></tr> <tr> <td>4</td><td>Elevato numero di <i>Short Dump ABAP</i> (relativi alla memoria)</td><td>Modifica temporanea dell'allocazione <i>heap</i> tramite <i>RSMEMORY</i> per programmi standard</td></tr> <tr> <td>5</td><td>Risorse <i>Dialog</i> insufficienti</td><td>Terminazione dei processi di lavoro <i>Dialog</i></td></tr> </tbody> </table> <p>Cloud ALM RUM – Monitoraggio manuale solo una volta al giorno da EU</p> <ul style="list-style-type: none"> Configurazione della funzionalità <i>RUM</i> nel <i>CALM</i> del cliente. Viene implementata solo la funzionalità standard – fino a 30 elementi di servizio. Configurazione del monitoraggio manuale <i>Real User Monitoring</i> per <i>S/4HANA PCE</i> – solo 1 sistema di produzione. <ul style="list-style-type: none"> Fino a 10 connessioni HTTPS Fino a 10 <i>WebService</i> Fino a 5 connessioni UI5 Fino a 5 <i>SOAP Webdynpro</i> 	#	Descrizione Alert	Attività di Remediation	1	Carico utente elevato su sistema o istanza ABAP	Terminazione dell'attività utente relativa a <i>statement</i> costosi identificati	2	Elaborazione <i>Enqueue</i>	Cancellazione dei <i>lock Enqueue</i>	3	Uso elevato della memoria ABAP	Modifica temporanea dell'allocazione <i>heap</i> o memoria estesa tramite <i>RSMEMORY</i>	4	Elevato numero di <i>Short Dump ABAP</i> (relativi alla memoria)	Modifica temporanea dell'allocazione <i>heap</i> tramite <i>RSMEMORY</i> per programmi standard	5	Risorse <i>Dialog</i> insufficienti	Terminazione dei processi di lavoro <i>Dialog</i>
#	Descrizione Alert	Attività di Remediation																		
1	Carico utente elevato su sistema o istanza ABAP	Terminazione dell'attività utente relativa a <i>statement</i> costosi identificati																		
2	Elaborazione <i>Enqueue</i>	Cancellazione dei <i>lock Enqueue</i>																		
3	Uso elevato della memoria ABAP	Modifica temporanea dell'allocazione <i>heap</i> o memoria estesa tramite <i>RSMEMORY</i>																		
4	Elevato numero di <i>Short Dump ABAP</i> (relativi alla memoria)	Modifica temporanea dell'allocazione <i>heap</i> tramite <i>RSMEMORY</i> per programmi standard																		
5	Risorse <i>Dialog</i> insufficienti	Terminazione dei processi di lavoro <i>Dialog</i>																		
Gestione Deployment - SolMan Charm	DP3	<p>Configurazione di <i>ChaRM</i> o <i>CTS+</i> nell'ambiente <i>SAP Solution Manager</i> del cliente (configurazione standard).</p> <p>Abilitazione all'uso di <i>ChaRM</i> o <i>CTS+</i>. Manutenzione continua di <i>ChaRM</i> o <i>CTS+</i>, che include:</p> <ul style="list-style-type: none"> creazione e aggiornamento di <i>branch</i>, creazione e aggiornamento di release/cicli di rilascio correzione di bug nella configurazione esistente di <i>SAP Solution Manager</i> 																		
Application operations	A1	Anno 1: 24 ticket. Anni successivi: 48 ticket/anno.																		
BTP Core operations	A3	Numero di account globali BTP: 1. Numero di <i>subaccount</i> : 3																		
Cloud ALM	O2	SAP fornirà supporto per <i>SAP CLOUD ALM TENANT</i> per le attività di responsabilità del cliente.																		

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

Test di Regressione	T1	Ciclo di test di regressione per anno: 1. Transazioni: fino a 200. Strumento di test: SAP <i>SolMan</i> o <i>Cloud ALM</i> .
Test di Performance	P1	10 processi di business

I servizi applicativi identificati potranno essere rimodulati, tramite *change request*, in maniera flessibile per indirizzare eventuali variazioni delle esigenze.

4.4.1.4 Servizi aggiuntivi a copertura di eventuali richieste al momento non pianificabili

Per consentire a Sogei di rispondere in maniera tempestiva ad eventuali esigenze al momento non pianificabili (es. Backup straordinario – *Customer Data handover* – *Additional Service*) dovrà essere previsto un monte valore di servizi opzionali acquistabili tramite *service request* come di seguito rappresentato:

Tipologia	Numero Service Request	Stima Valore Unitario
Servizi Aggiuntivi	50	2.000 Euro ad intervento

Sogei dovrà poter chiedere tali servizi opzionali e dovrà poterli chiedere tramite *Service Request* sul portale “*SAP for ME*”; a fronte di ciascuna richiesta verranno comunicati a Sogei il costo unitario della richiesta e l’effort di esecuzione.

Si riportano di seguito, a titolo di esempio, i principali servizi di possibile interesse per il contesto Sogei.

Codice Identificativo	Task	Tipologia
BASIC_1.8.13	<i>Data handover</i> dal service provider al cliente - <i>additional request</i>	<i>Additional Service</i>
INFRA_1.8.10	Esecuzione di backup eccezionali ad hoc su richiesta	<i>Additional Service</i>
HANA_1.1.35	Partizionamento delle tabelle (esecuzione tecnica) - <i>additional requests</i>	<i>Additional Service</i>

La lista di tali servizi attivabili tramite *service request* è riportata nella matrice *Roles & Responsibilities* (https://www.sap.com/about/agreements/policies/hecs-services.html?sort=latest_desc&tag=language%3Aenglish&tag=agreements%3Aproduct-policy%2Fecs%2Froles-and-responsibilities&pdf-asset=3e742235-cc7e-0010-bca6-c68f7e60039b&page=1)

4.4.2 Servizi Specialistici SAP Premium Engagement/Quality Assurance

Al fine di supportare Sogei nell’esecuzione ed il coordinamento delle attività di risoluzione delle tematiche di *operation* e/o per l’indirizzamento di esigenze progettuali, la soluzione SAP CDC

per Sogei dovrà prevedere un servizio specialistico SAP di *quality assurance* per la durata di 24 mesi.

Tale servizio interverrà sulle seguenti aree:

- *roadmap* evolutiva per il *porting* funzionale delle soluzioni SAP S/4HANA a SAP CDC;
- *shift* applicativo delle soluzioni SAP S/4HANA a SAP CDC;
- integrazione della SAP CDC con gli strumenti di monitoraggio del cliente;
- linee guida per il *change management* e gestione ed ottimizzazione delle procedure di test;
- linee guida per l'analisi *end to end* dei processi implementati su soluzioni SAP.

Il servizio SAP *Premium Engagement* prevede un coinvolgimento continuativo del team SAP per un periodo di erogazione di 24 mesi a partire dalla sottoscrizione del contratto. I servizi SAP *Premium Engagement* sono eseguiti dal centro di competenza SAP sulle tematiche definite nel perimetro, e/o altre richieste del cliente, attraverso servizi standard SAP o servizi personalizzati per Sogei. A valle del singolo servizio o dell'attività presa in carico e condotta dal team SAP, il team stesso provvederà a stilare e condividere con il cliente un documento di dettaglio delle analisi eseguite, le proposte di soluzione identificate, etc. (es. dettaglio delle *issue* rilevate con la rispettiva soluzione, dettaglio del processo analizzato e indicazioni di tuning specifico, etc.).

Si riportano di seguito le principali schede servizio identificate per il contesto Sogei che si prevede di erogare nell'arco temporale della sottoscrizione:

Declinazione degli indirizzi strategici in piani operativi

Area	Descrizione	Coninvolgimento SAP	Coninvolgimento Sogei
------	-------------	---------------------	-----------------------

Team SAP per la declinazione degli indirizzi strategici in piani operativi	Roadmap evoluzione SAP BO - Supporto nella definizione dell'evoluzione degli ambienti SAP BO	- Studio fattibilità e <i>roadmap</i> - Analisi dell'attuale architettura per le istanze SAP BO assolute ed IGRUE - Verifica materiali e compatibilità con i sistemi affrontati	- Condivisione dei piani di Progetto sulle componenti definite nel perimetro - Partecipazione attiva di risorse durante le attività di analisi dei requisiti - Discussione o condivisione dell'architettura tecnica AS-IS - Pianificazione attività in base alla roadmap TO-BE definita - Condivisione del contingentamento
	Roadmap evoluzione IGRUE - Supporto nella definizione dell'evoluzione degli ambienti SAP IGRUE	- Analisi di razionalizzazione dell'architettura AS-IS - Analisi ed individuazione di eventuali <i>Quick Win</i> per la piattaforma IGRUE - Definizione scenario TO-BE e <i>Top Design</i> architetturale	
	Indirizzamento di ulteriori esigenze progettuali e/o aree specifiche - Risorse specializzate per tematiche cross area e soluzioni (es. SAC - <i>Planning Area</i> , Revisione codice avanzato)	- Indirizzamento esigenze specifiche - Analisi di dettaglio su tematiche specifiche - Coinvolgimento risorse/attivazione servizi specialistici	
	Figura di raccordo e coordinamento tra il team Sogei ed il team dedicato CDC	- Condivisione risultati e rilascio documentazione a SOGEI e <i>System Integrator</i>	

Testing Optimization

Area	Descrizione	Coninvolgimento SAP	Coninvolgimento Sogei
Testing Optimization (Tricentis)	Sottoscrizione alla soluzione Tricentis per i moduli: <ul style="list-style-type: none"> SAP <i>Change Impact Analysis by Tricentis</i> <i>Tosca by Tricentis</i> SAP <i>Enterprise Performance Testing by Tricentis</i> 	Setup Configurazione del tool <i>Tricentis</i> per i moduli previsti	<ul style="list-style-type: none"> Partecipazione attiva di risorse durante le attività di testing (definizione ed esecuzione) Pianificazione delle attività e finestre di lancio (<i>performance test automation</i>) Analisi dei risultati ed indirizzamento di eventuali <i>feedback</i> Coinvolgimento di team interni/<i>System Integrator</i> per favorire l'adozione/l'estensione dell'utilizzo degli strumenti (eventuale adeguamento delle procedure Sogei)
	Performance Test Supporto all'azione del prodotto <i>Tricentis</i> per le funzionalità relative al performance test	Performance Test (Ricorrente) <ul style="list-style-type: none"> Creazione e caricamento base dati e casi di test in affiancamento a Sogei <i>Run test</i> di carico in affiancamento a Sogei 	
	Change Impact Analysis/ Test automation Supporto all'azione del prodotto <i>Tricentis</i> per le funzionalità relative all' <i>impact change analysis</i> e <i>test automation</i>	Regression Test (Ricorrente) <ul style="list-style-type: none"> Creazione e caricamento subset di test e automatizzazione in affiancamento a Sogei <i>Run test</i> su processi S/4HANA 	
		Knowledge Transfer Rilascio documentazione, manuali d'uso e risultati ad uso SOGEI e dei <i>System Integrator</i>	

Process repository and analysis

Area	Descrizione	Coninvolgimento SAP	Coninvolgimento Sogei
------	-------------	---------------------	-----------------------

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

<p>Process repository and analysis (SAP Signavio)</p>	<p>Sottoscrizione alla soluzione SAP Signavio per i moduli:</p> <ul style="list-style-type: none"> • SAP Signavio Process Manager • SAP Signavio Journey Modeler • SAP Signavio Process Intelligence and Insights • SAP Signavio Process Governance • SAP Signavio Collaboration Hub <p>Process Modeling</p> <p>Supporto all'esecuzione del process modeling relativo alle funzionalità di performance test.</p> <p>Process Analysis</p> <p>Supporto all'esecuzione dell'analisi del prodotto SAP Signavio per impact change analysis e test automation.</p>	<p>Setup</p> <p>Configurazione dei tool SAP Signavio per i moduli previsti.</p> <p>Process Modeling</p> <p>Creazione e caricamento di un processo E2E attraverso lo strumento Process Manager.</p> <p>Process Analysis</p> <ul style="list-style-type: none"> • Analisi approfondita per la definizione dello scenario attuale e dei dati da migrare • Configurazione dell'integrazione tra S4HANA e BPC • Scopi per l'analisi con SPCODEC2E • Esecuzione di un'analisi del processo per identificare eventuali punti di ottimizzazione <p>Knowledge Transfer</p> <p>Rilascio documentazione, manuali d'uso e risultati ad uso SOGEI e del System Integrator</p>	<ul style="list-style-type: none"> - Partecipazione attiva di risorse durante le attività di: • identificazione del processo e modellizzazione dello stesso • identificazione dei sistemi di backend in ambito per il rilascio dei dati • revisione e analisi dei risultati - Coinvolgimento team interni/System Integrator nelle fasi successive (eventuale adeguamento delle procedure Sogeti)
--	--	--	---

Monitoraggio applicazioni / Application Security Notes

Area	Descrizione	Coinvolgimento SAP	Coinvolgimento Sogeti
<p>Monitoraggio applicazioni</p>	<p>Critical Application Monitoring</p> <p>Attivazione del servizio di monitoraggio 24/7 delle applicazioni relative ai principali processi critici</p>	<ul style="list-style-type: none"> - Analisi delle applicazioni e delle interfacce afferenti a processi in ambito - Configurazione degli strumenti di monitoraggio per i Sistemi Core e 30 applicazioni - Definizione e automatizzazione delle soglie con invio automatico di segnalazioni - Gestione problematiche e apertura incidenti - Condivisione strumenti di monitoraggio 	<ul style="list-style-type: none"> - Partecipazione attiva di risorse durante l'identificazione delle applicazioni, la definizione delle soglie e della schedulazione - Condivisione nuovi requisiti di monitoraggio - Recepimento delle regole d'ingaggio
<p>Application Security Notes</p>	<p>Security Application</p> <p>Industrializzazione e implementazione delle note SAP di sicurezza</p>	<ul style="list-style-type: none"> - Condivisione dei modelli di installazione - Installazione delle note su tutti gli ambienti - Supporto durante le attività di manutenzione straordinaria per la gestione delle note di sicurezza - Condivisione delle attività svolte 	<ul style="list-style-type: none"> - Esecuzione, supporto e coordinamento delle fasi di testing delle note di sicurezza - Autorizzazione al rilascio in ambienti produttivi

Deployment Management

Area	Descrizione	Coinvolgimento SAP	Coinvolgimento Sogeti
------	-------------	--------------------	-----------------------

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogeti ID – 2925

Allegato 2 - Capitolato tecnico

Deployment Management	Attivazione ChaRM Industrializzare il ciclo di vita del SW SAP per semplificare i rilasci in produzione	Analisi - Analisi del processo di gestione delle <i>change request</i> sia nello scenario progetto che urgenze Setup ChaRM - Implementazione e configurazione del tool <i>ChaRM</i> - Definizione e condivisione dei Cicli di Manutenzione ed evoluzione del SW - Gestione ciclo di vita del codice custom Knowledge Transfer - Rilascio documentazione, manuali d'uso e risultati ad uso SOGEI e dei <i>System Integrator</i>	- Partecipazione attiva di risorse con competenze di sviluppo per la definizione dei cicli di vita del software - Condivisione dei piani dei Progetti interni, dei rilasci e delle nuove esigenze - Condivisione linee guida per l'utilizzo di <i>ChaRM</i> ai colleghi interni e fornitori
------------------------------	---	--	---

4.5 SAP CDC – Specificità del servizio Sogei

Data la rilevanza critico - strategica dei progetti in ambito (INIT – ReGiS), si riportano di seguito le specificità tecniche derivanti dalle linee guida architetture Sogei che dovranno essere soddisfatte dal servizio SAP CDC *tailored* per Sogei.

4.5.1 SAFEKEEPER - estensione finestra gestione per sistemi S/4HANA su SAP CDC

Il servizio *Safekeeper* consente l'estensione della finestra di gestione dei sistemi SAP S/4HANA su SAP CDC a fine del ciclo di manutenzione. Attualmente le installazioni SAP S/4HANA per i programmi INIT e Regis sono in versione 1909, versione non supportata in SAP CDC a meno dell'attivazione del servizio *Safekeeper*. Il servizio dovrà essere messo a disposizione fino al 31.12.2027, ed entro tale data è richiesto un upgrade ad una *release* compatibile con la SAP CDC (S/4HANA 2023 o S/4HANA 2025).

4.5.2 DISASTER RECOVERY

I servizi di *Disaster Recovery* dovranno prevedere RTO = 4h e RPO = 30 min per tutti gli ambienti produttivi. Il team *Operation/Architetture* di Sogei potrà richiedere test di *disaster recovery* aggiuntivi (nella SAP CDC dovranno essere compresi due test di DR l'anno) attraverso l'apertura di una *service request*.

Inoltre, per supportare i test di DR senza impattare il servizio degli ambienti produttivi S/4HANA INIT, BW/4HANA INIT, S/4HANA ReGiS, BW/4HANA ReGiS, SAP BO (unico ambiente in DR da riutilizzare per i vari *landscape BO*), SAP ADS e SAP PO la *reference architecture* certificata da SAP per la CDC prevede database aggiuntivi sul sito di DR.

L'ambiente *sandbox* di SAP BO verrà utilizzato per testare le diverse installazioni di Sogei e sarà ripristinato, dal sito primario, in base alle esigenze, al fine di verificare la corretta apertura dei report valorizzati con i dati dei sistemi sorgente. SAP BO, infatti, non memorizza dati nel proprio database: questi verranno recuperati direttamente dai sistemi sorgente, che dovranno essere accessibili durante l'esecuzione del test di *Disaster Recovery* (DR).

4.5.3 LOGGING / AUDITING

Per ogni componente all'interno della SAP CDC dovrà essere eseguita la raccolta, l'archiviazione e l'analisi dei log dell'infrastruttura e della sicurezza. I *trigger* di minaccia e gli avvisi degli eventi raccolti all'interno dei log, dovranno essere gestiti mediante specifici tool; attraverso il servizio chiamato LogServ, dovranno essere disponibili per Sogei, tramite un syslog, le informazioni di *logging/auditing* relative ai vari livelli oltre lo strato applicativo (OS, DB, infra) da cui sarà possibile alimentare il *SIEM/Log Management* Sogei.

Lo scopo del servizio LogServ è quello di fornire tutte le informazioni necessarie al monitoraggio e all'auditing delle attività che vengono svolte a sistema. Il servizio garantisce l'accesso ai log in *near-real time* su diversi livelli sfruttando i meccanismi nativi di *logging* delle rispettive componenti rendendoli disponibili attraverso *syslog* verso l'esterno (es. *SIEM*, software deputati all'analisi delle attività svolte). I log che verranno raccolti saranno di diversa natura ed includono log infrastrutturali ed applicativi come ad esempio gli audit log di *HANA*.

La definizione degli accessi, e di conseguenza del *logging* e *tracking* a livello applicativo, è gestita da Sogei che potrà definire in autonomia o con l'eventuale supporto di SAP ruoli, *auditing* e livelli di accesso, inclusa l'eventuale integrazione con un *SIEM* esterno. Il supporto di personale SAP per la definizione, la configurazione e l'*hardening* di queste componenti potrà essere richiesto a discrezione di Sogei.

L'approccio consentirà a Sogei di avere il pieno controllo sullo strato applicativo SAP, visto che l'accesso al *client* applicativo per il personale SAP è consentito solo su esplicita autorizzazione Sogei.

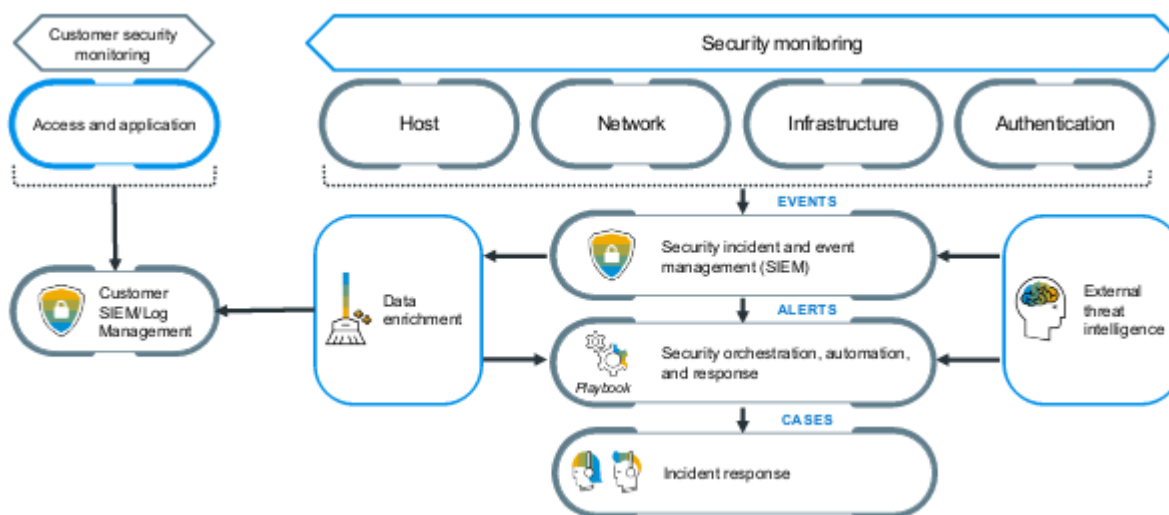


Figura 6 - Security Monitoring

4.5.4 MONITORAGGIO CDC e STRUMENTI A SUPPORTO DELLE OPERATION

Per garantire a Sogei un'efficienza operativa anche nel nuovo modello, la struttura *Operation/Architetture* di Sogei dovrà disporre all'interno della *reference architecture* e sottoscrizione SAP CDC di diversi strumenti a supporto del monitoraggio del servizio:

- Accesso al database – Sogei dovrà avere a disposizione le credenziali di accesso sul *systemDB* e sul *tenantDB* con privilegi di sola lettura;
- Tracciatura eventi e log generati dai sistemi – I log infrastrutturali e applicativi dovranno essere inoltrati al *SIEM/Log Management Sogei*;
- IAAS logs, VM per attività day-by-day – La *reference architecture* certificata da SAP dovrà prevedere una macchina virtuale (VM) come server IaaS dove Sogei potrà accedere ai log dei sistemi della SAP CDC;
- ABAP OS Command – attraverso le transazioni standard (es. *ST06*, programma *RSBCOS0*), dovrà essere consentito a Sogei di accedere in visualizzazione ai processi principali in esecuzione, parametrizzazioni del SO, consumo risorse, file system, etc.;
- System Monitoring / Alerting SolMan – dovrà essere prevista l'attivazione del *System Monitoring* e relativo *alerting* all'interno del *Solution Manager* di Sogei che dovrà includere anche il monitoraggio delle transazioni critiche;
- Integrazione monitoraggio con la Service Control Room – dovrà essere prevista l'integrazione degli eventi catturati dal *Solution Manager* verso la *Service Control Room* Sogei;
- SAP for Me – Cruscotto di monitoraggio per i servizi della SAP CDC;
- Conduzione Sessione remota ad hoc SAP/Sogei – dovrà essere garantito il supporto di una risorsa SAP dedicata (TSM) per verifiche puntuali su SAP CDC attraverso *screen sharing*;
- Attivazione "Service Continuity Plan" (vedi Allegato 1).

La struttura *Operation/Architetture* di Sogei dovrà avere piena visibilità sulle configurazioni e le parametrizzazioni a livello di SAP *HANA* e di tenant attraverso lo strumento DBA Cockpit, disponibile di default su tutti gli ambienti. Il team Sogei, attraverso le transazioni standard (es. *ST06*, programma *RSBCOS0*), dovrà poter accedere in visualizzazione ai processi principali in esecuzione, parametrizzazioni del SO, consumo risorse, *file system*, etc.

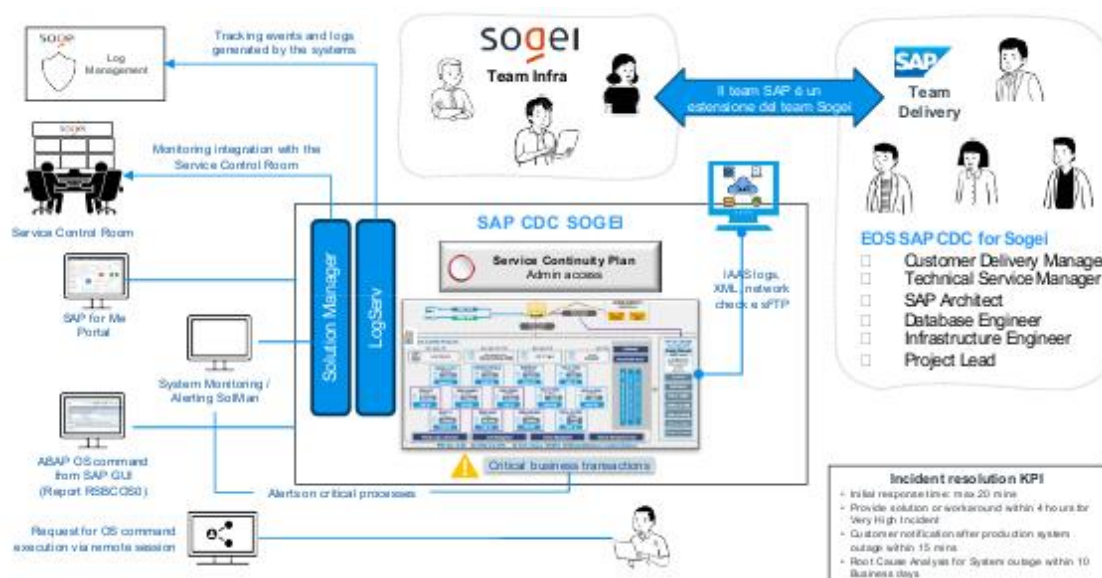


Figura 7 - Monitoraggio CDC e strumenti a supporto delle Operations

Il *Technical Service Manager* (TSM) sarà la risorsa che lavorerà a stretto contatto con il team infra/operation per affiancare Sogei nelle attività quotidiane e nel supportare le analisi di *troubleshooting*.

Il *Technical Service Manager* (TSM) dovrà essere quindi disponibile per organizzare e facilitare sessioni di condivisione dello schermo per effettuare analisi approfondite a livello del sistema operativo.

Tale servizio, incluso nella SAP CDC, estenderà il task della matrice RACI “BASIC_1.1.14 - *Assist customers with tasks in their area of responsibility if OS access is required*” superando le limitazioni sul numero di esecuzione e consentirà a Sogei di ingaggiare direttamente il TSM senza vincoli di preventiva apertura di service *request/ticket*.

4.5.5 IAAS logs, VM per attività day-by-day

Per garantire a Sogei un'efficienza operativa anche nel nuovo modello, in particolare nella gestione di applicazioni basate su sistemi cross CDC e non (es. integrazioni BOBS), la *reference architecture* certificata da SAP dovrà prevedere una macchina virtuale (VM) come server IaaS dove Sogei potrà entrare con le credenziali di root.

La VM IaaS sarà nella stessa sottorete degli altri sistemi SAP. Pertanto, la VM IaaS può essere utilizzata per raccogliere statistiche di rete.

La VM IaaS dovrà consentire a Sogei di avere visibilità dei File System in uso all'interno della SAP CDC, dal quale sarà possibile accedere in read-only ai log di sistemi e in alcuni casi di avere il controllo diretto di file specifici dell'applicazione (es. file xml SAP Business Object).

Tecnicamente tale “IaaS VM”:

- Farà il '*mount*' dei *filesystem* dei vari *host* che consentirà l'accesso diretto ai file dei vari sistemi;
- Dove necessario sarà possibile accedere ai *filesystem* di cui sopra in *read-write* per consentire la modifica diretta dei file di configurazione (esempio i file XML di *BOBJ*);
- Sarà attivato su questa 'IaaS VM' un servizio sFTP che consentirà a sistemi esterni a tale 'IaaS VM' (per esempio un laptop) di accedere a tutti i file senza collegarsi alla 'IaaS VM';
- La configurazione di rete di questa 'IaaS VM' sarà speculare a quella di tutti gli altri *host* presenti, in modo tale da rendere significativa un'analisi lato *networking* (es. *traceroute*) fatta da questa macchina per un eventuale *troubleshooting* della componente rete.

La "IaaS VM" dovrà consentire a Sogei:

- L'esecuzione di tutti i comandi che interagiscono con file (es: *cat*, *find*, *grep*, *awk*, etc.), di fatto l'esecuzione di tali comandi dalla 'IaaS VM', avendo accesso ai *filesystem* è equivalente all'esecuzione diretta sui server;
- Tali comandi sui file saranno eseguibili anche dagli *host* esterni tramite l'uso di sFTP che consente a Sogei di avere la visibilità dei *filesystem* anche scaricando eventualmente i file in locale;

Per i due punti di cui sopra, di conseguenza, sarà possibile:

- apportare modifiche ai file di configurazione in modo diretto sia dalla 'IaaS VM' che da remoto via SFTP
- Poter eseguire comandi di rete direttamente dalla 'IaaS VM' (come, ad esempio, il *curl*) visto che la 'IaaS VM' avrà un indirizzamento nella stessa *subnet* degli *host* SAP CDC garantendo di avere un contesto di rete significativo per il *troubleshooting*.

Per quanto riguarda i comandi di monitoraggio dei processi (es: *ps*, *top*) che per loro natura non possono essere eseguiti da sull' "IaaS VM" valgono i seguenti punti a supporto dell'operatività quotidiana:

- lo stato dei processi di una macchina Linux si può avere anche attraverso l'accesso al *filesystem* */proc* che rappresentano in formato file lo stato del sistema, cosa che potrà essere richiesta come ulteriore *export* remota;
- le informazioni sullo stato dei sistemi saranno disponibili sulle dashboard in *near real-time* del Solution Manager dove è prevista anche l'attivazione delle notifiche di *alert* per superamento delle soglie di utilizzo delle risorse di sistema;
- qualsiasi altra attività da eseguire direttamente sul sistema sarà possibile richiederla al TSM (senza necessità di una *service request*) per eseguire una sessione remota e

lanciare i comandi desiderati sui sistemi operativi; il TSM sarà di fatto una risorsa dedicata a Sogei.

4.5.6 BACKUP

Le policy di *backup*, i cui dettagli sono riportati nella tabella seguente, prevedono che i *backup* dovranno essere creati nel sito primario e tutte le copie saranno archiviate nel sito primario e replicate nel sito secondario. Tutti i *backup* dovranno essere crittografati e memorizzati nello *storage* adibito allo scopo nella SAP CDC,

Specifica	Database/log	Produzione File System	Database/log	Non produttivo File System
Frequenza	Full giornaliero	Full mensile	Full giornaliero	Full mensile
	Log come da standard di prodotto	Incrementale giornaliero	Log come da standard di prodotto	Incrementale giornaliero
sRetention	30 giorni	2 mesi	14 giorni	2 mesi
Location	Sito primario e secondario	Sito primario e secondario	Sito primario e secondario	Sito primario e secondario

La *reference architecture* SAP CDC prevede la replica di una copia dei *backup*, nel formato del *backup* SW previsto nella SAP CDC, su un media (es. NFS) messo a disposizione da Sogei. La replica dei *backup* su media esterno dovrà essere compresa nel servizio. Sarà cura di Sogei predisporre un'infrastruttura HW/SW adeguata all'eventuale *restore* dei *backup* replicati.

4.5.7 SCHEDULAZIONE DEI JOB

La schedulazione dei job in Sogei è gestita in maniera centralizzata, attraverso il software TWS, che prevede una componente server centrale e il *deploy* di un *agent* per la gestione dei diversi tipi di applicativi (es. SAP, etc.). La configurazione attuale per gli ambienti SAP prevede l'installazione dell'*agent* sul server SAP SCS (SAP *Central Services*), configurato per comunicare con le diverse istanze SAP (es. *S/4HANA*, *BW/4HANA*, etc.).

Nel contesto SAP CDC dovrà essere possibile continuare ad utilizzare l'attuale *agent*, che resta installato sul server SAP SCS Sogei (HW Sogei attuale/alternativo e non in ambito SAP CDC), modificando solo il file di *properties* per collegare l'*agent* stesso con le soluzioni migrate in SAP CDC. In questo modo l'impatto legato al progetto di migrazione viene minimizzato nel contesto schedulatore e mantiene l'iso-funzionalità rispetto allo scenario sopra descritto e piena autonomia nella gestione da parte della struttura.

In alternativa, lo stesso *agent* potrà essere installato, configurato e gestito da Sogei su server dedicato IaaS all'interno della *reference architecture* definita per la SAP CDC, mantenendo sempre l'iso-funzionalità rispetto allo scenario sopra descritto.

4.5.8 VULNERABILITY ASSESSMENT

Sogei dovrà avere la possibilità di eseguire una volta l'anno *vulnerability/ penetration test* in linea con le indicazioni riportate nella nota SAP <https://me.sap.com/notes/3080379>.

Con frequenza trimestrale dovranno essere resi disponibili a Sogei i report di *Vulnerability Assessment* contenenti le vulnerabilità note (CVE) presenti nei sistemi, per i servizi ricompresi nel Perimetro Nazionale di Sicurezza Cibernetica gli stessi dovranno essere forniti nel formato richiesto dall'Agenzia della Cybersecurity Nazionale.

Resta comunque inteso che, all'interno del servizio SAP CDC, potranno essere consultati sul portale SAP Trust Center (link di seguito: https://www.sap.com/about/trust-center/certification-compliance/compliance-finder.html?sort=latest_desc&tag=compliance-document:compliance-offering/soc-2) il report di conformità SOC 2, contenente informazioni dettagliate sul sistema di controllo relativo alla sicurezza, alla disponibilità, all'integrità del trattamento o alla riservatezza dei dati.

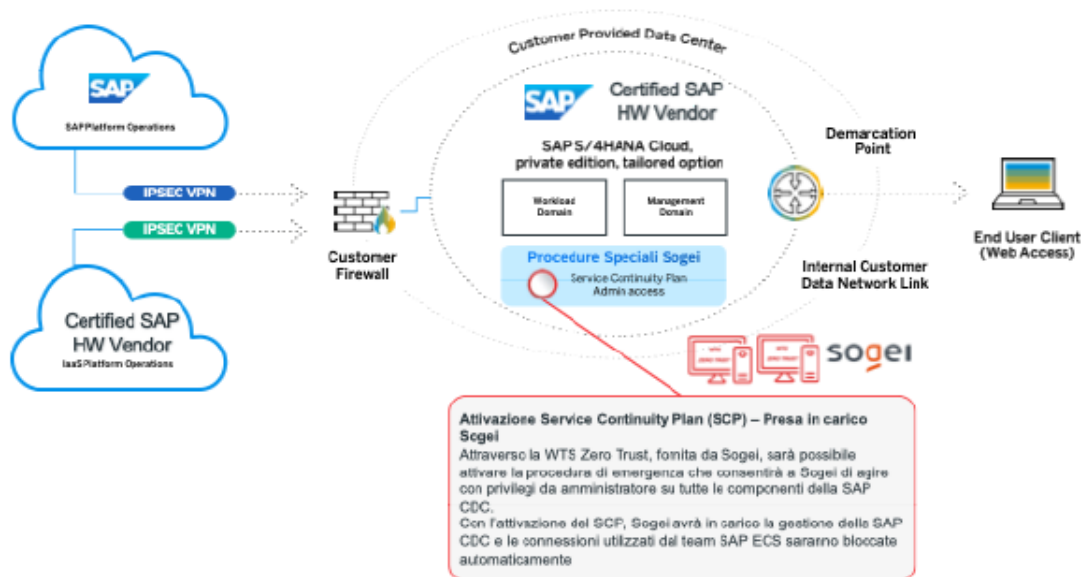
4.5.9 GESTIONE INCIDENTI DI SICUREZZA

È necessario che SAP si impegni a notificare tempestivamente, senza ingiustificato ritardo, qualsiasi evento che possa comportare un incidente di sicurezza per Sogei. In tal caso, SAP concorda con Sogei i flussi di comunicazione e reportistica in caso di incidente e supporta la stessa nelle attività di indagine e analisi post-incidente.

SAP in aggiunta si impegna alla disclosure di incidenti informatici subiti da sé stesso o dalla sua *supply chain* nel momento che si dovesse prospettare un possibile impatto per Sogei.

4.5.10 PROCEDURA SERVICE CONTINUITY PLAN

Nell'ambito della *reference architecture* SAP CDC dovrà essere prevista la possibilità che Sogei prenda in carico i sistemi attraverso l'attivazione della procedura "Service Continuity Plan" (vedi Allegato 1).



Le casistiche di attivazione del servizio sono legate al rispetto di quanto espresso all'interno del riferimento normativo decreto-legge 21 settembre 2019, n. 105 che definisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e sancisce le responsabilità di Sogei di tutelare i propri beni ICT il cui malfunzionamento causerebbe l'interruzione totale o una compromissione dei servizi offerti alla Pubblica Amministrazione.

In tale contesto l'attivazione del *Service Continuity Plan* è un atto formale che prevede la comunicazione, quando possibile, da parte di Sogei verso SAP della necessità di attivare tale piano e della motivazione per cui Sogei intende attivarlo.

Infine, nel seguente sinottico vengono riepilogate le principali caratteristiche delle linee guida *Service Continuity Plan*.

Figura 8 - Service Continuity Plan



Tipologia Accesso	<ul style="list-style-type: none"> Accesso con privilegi di amministratore su tutta l'infrastruttura SAP CDC
Meccanismo Attivazione	<ul style="list-style-type: none"> Attivazione a discrezione di Sogei tramite WTS Zero Trust (messa a disposizione da Sogei) con blocco contestuale delle VPN utilizzate dal team di supporto SAP ECS.
Responsabilità	<ul style="list-style-type: none"> Sogei avrà in carico la gestione della SAP CDC Sogei sarà responsabile del auditing delle attività effettuate sul client Sogei. SAP è esentata dal rispetto delle SLA e degli altri obblighi contrattuali
Modalità di rientro nel servizio standard	<ul style="list-style-type: none"> La ripresa in carico del servizio da parte di SAP è condizionata da assessment di valutazione, delle modifiche effettuate da Sogei, con lo scopo di determinare gli interventi di bonifica e garantire il rientro alla gestione standard e agli obblighi contrattuali

Figura 9 - Linee Guida Service Continuity Plan

Si precisa che Sogei metterà a disposizione due client WTS che dovranno avere le caratteristiche *Zero Trust*, ovvero sarà possibile eseguire audit e/o la condivisione della registrazione delle attività eseguite.

4.5.11 ENCRYPTION

All'interno della *reference architecture* SAP CDC, la crittografia *data-at-rest* è implementata su più livelli; la crittografia è attiva sullo storage e sul database attraverso funzionalità native. In particolare, per il database viene applicata la crittografia sulle strutture dati e log attraverso funzionalità native SAP HANA.

La crittografia all'interno della SAP CDC garantisce che:

- I volumi di dati non siano accessibili in chiaro dall'infrastruttura;
- Chiunque riesca ad accedere ai volumi di dati sul disco tramite OS non riesca a vedere i dati;
- Il *backup* per essere utilizzato richiede l'inserimento della chiave crittografica, oltre al SW di *backup* per la *restore*.

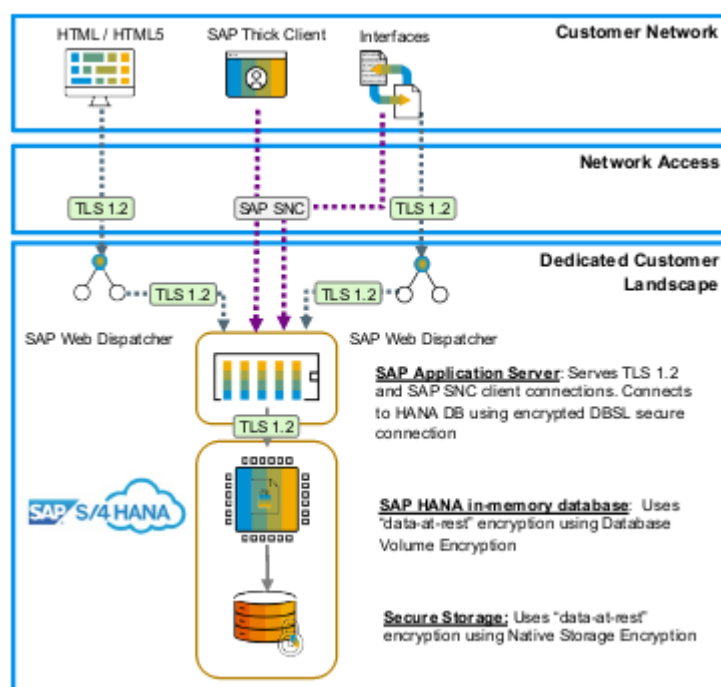


Figura 10 - Crittografia SAP CDC

All'interno della *reference architecture* SAP CDC, secondo le *best practices* suggerite da SAP, è implementata la crittografia *data-in-transit* per tutte le connessioni dei client verso i sistemi SAP attraverso la protezione del traffico HTTP con protocollo minimo TLS 1.2 e cifratura.

Per quanto riguarda il soddisfacimento dei requisiti espressi da Sogei, relativamente alla gestione delle chiavi di crittografia, il servizio supporta gli scenari *Bring Your Own Key* (BYOK) che consente la gestione delle chiavi da parte di Sogei in un HSM o KMS esterno supportato.

Si specifica che, nel ciclo di vita della chiave, gestita attraverso HSM/KSM esterno, – dalla generazione alla rotazione – e nelle attività di amministrazione dei sistemi, non è previsto che alcun soggetto terzo entri in possesso della chiave di crittografia.

4.5.12 ACCESSO AL DATO IN SAP CDC

Nella seguente figura viene condiviso il modello di accesso alle applicazioni SAP:

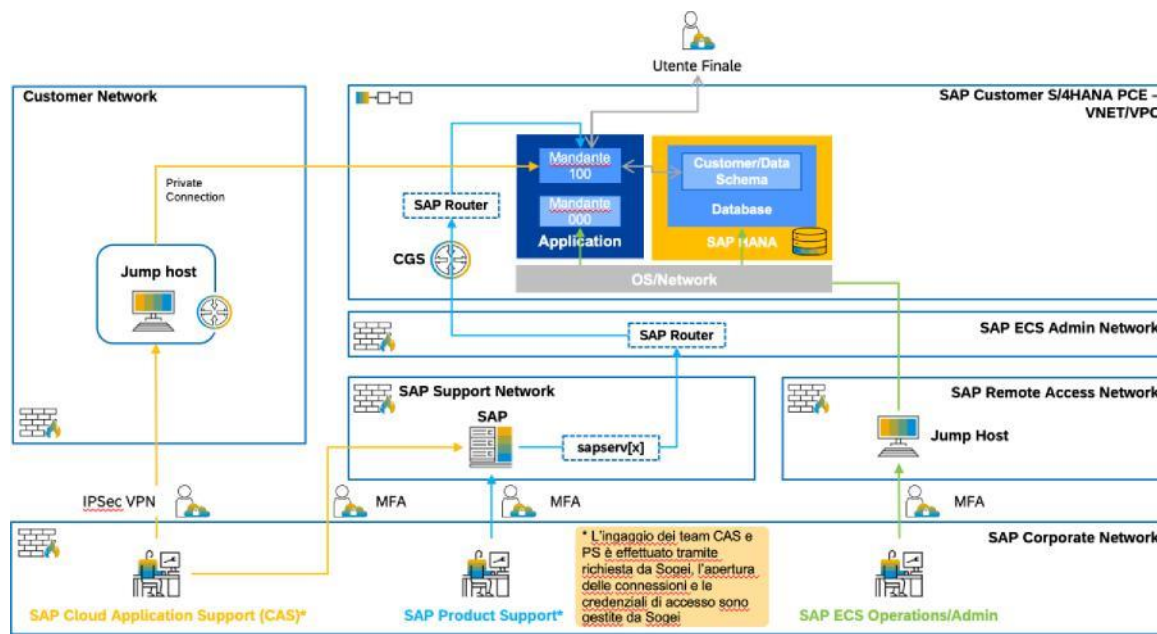


Figura 11 - Accesso al dato nella SAP CDC

Nella seguente tabella vengono riportate le possibili casistiche di accesso definite in base alla tipologia di servizio/supporto richiesto.

	SAP ECS (verde)	SAP CAS (giallo)	SAP Product Support (azzurro)
Tipologia attività	Supporto operativo di <i>system admin</i> dei sistemi SAP	Supporto operativo di secondo livello nella gestione dei sistemi SAP	Supporto specialistico richiesto in caso di incidenti applicativi e/o emergenze
Modalità di ingaggio	Nessun ingaggio richiesto, il team SAP ECS lavora costantemente sui sistemi SAP per il supporto alla gestione delle <i>operations</i>	Ingaggio su richiesta da parte di Sogei. Per questa attività è necessario aprire una <i>service request</i> e la connettività puntuale verso il sistema SAP.	Ingaggio su richiesta da parte di Sogei. Per questa attività è necessario aprire un <i>incident</i> applicativo e la connettività puntuale verso il sistema SAP.
Modalità di accesso	Accesso tramite Jump Host all'interno della SAP CDC via rete di amministrazione dedicata basata su VPN	Accesso tramite Jump Host gestito da Sogei oppure tramite <i>saprouter</i> attraverso rete Sogei	Accesso tramite il <i>saprouter</i> attraverso rete Sogei

Recupero Credenziali	Le credenziali per la gestione dei sistemi sono recuperate da uno strumento centrale CAM e richiede un processo approvativo definito. Approvazione Sogei per SAPHANADB.	Le credenziali e le autorizzazioni sono definite da Sogei	Le credenziali e le autorizzazioni sono definite da Sogei
Accesso al dato applicativo	No. SAP ECS accede solo al client tecnico 000 e non ha accesso ai dati di business residenti nel customer schema	Si, dietro consenso da parte di Sogei e apertura della connessione remota/WTS al sistema SAP	Si, dietro consenso da parte di Sogei e apertura della connessione remota al sistema SAP

Come rappresentato in tabella, l'accesso al dato applicativo da parte del team SAP ECS non dovrà essere consentito in alcun modo; questo potrà essere garantito dall'utilizzo dello strumento *SAP User Lifecycle Tool* (CAM), che dovrà essere invocato ogni qualvolta che si vorrà accedere ai sistemi SAP.

La postazione Jump Host utilizzata dal team ECS segue il principio *zero trust*, ovvero la sessione dell'operatore sarà registrata, e dovrà rispettare i principi di sicurezza rappresentati nella seguente figura.

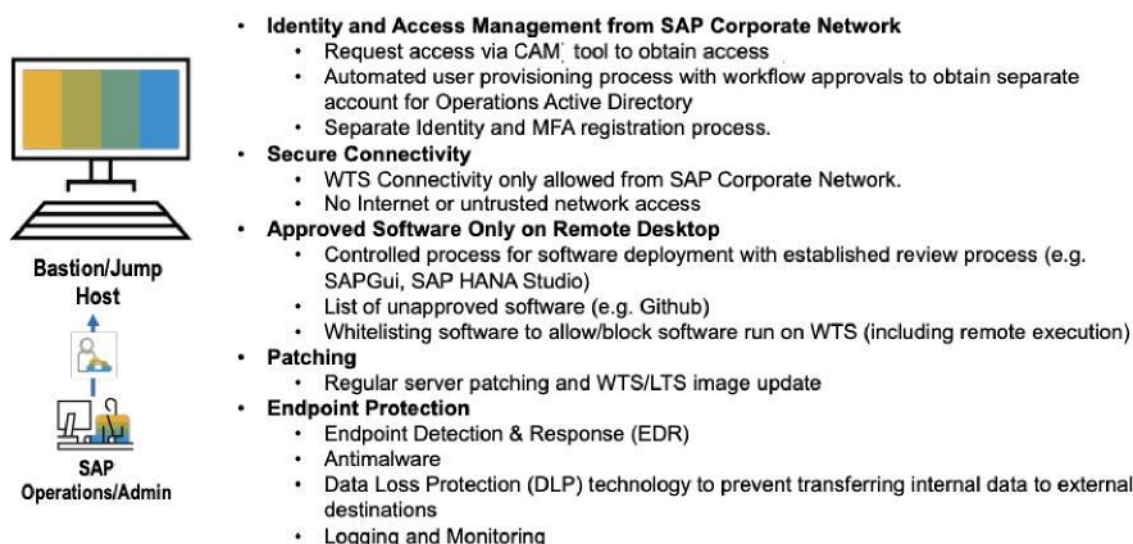


Figura 12 - Postazione Jump Host

Tutte le password dei sistemi della SAP CDC non dovranno essere disponibili agli operatori ECS, ma dovranno essere gestite attraverso lo strumento CAM. Il CAM quando verrà invocato dall'operatore, innescherà un processo approvativo registrato, che fornirà un accesso temporaneo (*time-based*) diretto alla risorsa richiesta, solo dopo aver verificato il profilo autorizzativo.

Vale sottolineare che nell'adozione della SAP CDC è possibile identificare due momenti principali:

- Attività di migrazione: in cui le password dovranno essere assegnate al team che esegue la migrazione (Sogei /servizi SAP/system integrator);

- Successivamente, nella fase di *onboarding* del servizio, le password dovranno essere messe in sicurezza e dovranno essere gestite attraverso strumenti che non consentiranno al team SAP ECS di reperire la password (CAM).

Lo strumento CAM in questione ha le seguenti caratteristiche:

- Strumento utilizzato da SAP per gestire l'accesso degli utenti ai sistemi del cliente: applicazioni, database e sistema operativo;
- Applicazione di *policy* basate sui ruoli con privilegi minimi e segregazione dei compiti time-based;
- Reset automatico delle password dopo il *check-out* dell'operatore;
- Tutte le richieste vengono approvate dal personale autorizzato;
- Il processo di richiesta viene registrato con la traccia di controllo (audit) per il non ripudio;
- Processo formale di revisione dell'accesso degli utenti.

Si riporta di seguito il processo approvativo che viene innescato sul CAM quando si richiedono le credenziali di accesso al sistema.

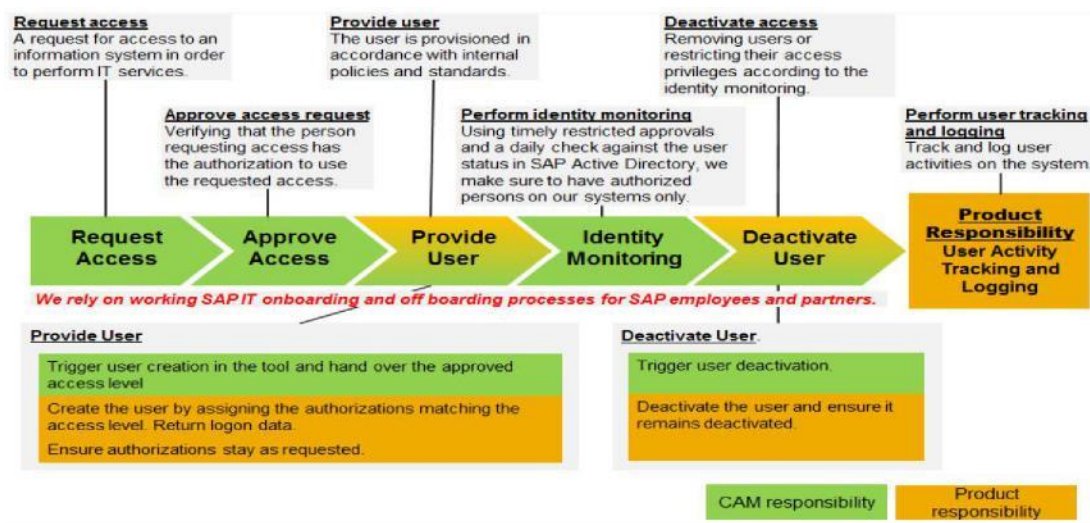


Figura 13 - Processo approvativo quando si richiedono le credenziali

Il processo di richiesta dell'autorizzazione e l'esecuzione delle attività sono registrate rispettivamente sul CAM e sul sistema su viene effettuato l'accesso. Tali log sono inoltrati e disponibili al *SIEM/Log Management* di Sogei.

A titolo esemplificativo, viene riportata nella seguente immagine, il *workflow* di esecuzione di una richiesta di accesso amministrativo a SAP HANA, dove si evince che non è possibile accedere al customer schema.

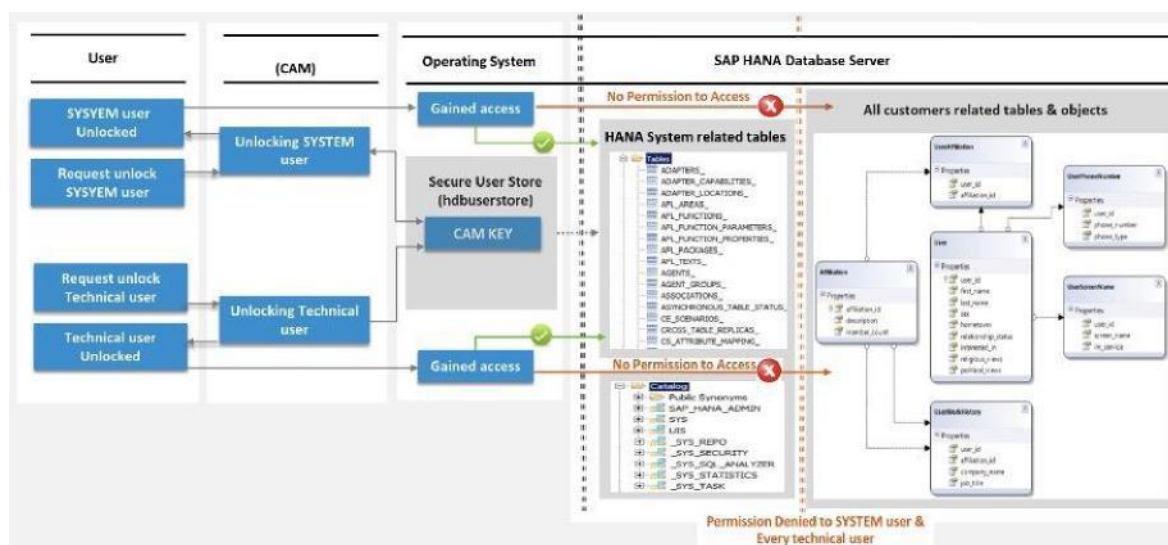


Figura 14 - workflow di esecuzione di una richiesta di accesso amministrativo a SAP HANA

Per quanto riguarda i team CAS e Product Support, dovrà essere Sogei ad aprire la connettività verso i propri sistemi e definire credenziali e autorizzazioni da condividere con i due team per consentire l'accesso al sistema SAP sul mandante produttivo, coerentemente con i modelli di accesso già in essere oggi nell'implementazione attuale.

La gestione dell'accesso al dato è conforme alle normative in materia ISO/IEC 27001 e SOC2 che vengono revisionate annualmente seguendo un processo formale di audit esterno.

Gli strumenti e la procedura sopra descritta, nella piena conformità delle normative riportate, dovrà garantire il pieno rispetto della sovranità del dato consentendo a Sogei di accedere a tutte le informazioni con un modello analogo a quello *OnPremise* attualmente in essere.

4.5.13 Gestione lifecycle utenza SAPHANADB

Per indirizzare il requisito relativo alla sovranità del dato nel contesto SAP CDC dovrà essere implementata la seguente procedura speciale per Sogei:

- In relazione all'utente tecnico *SAPHANADB*, SAP definirà un processo ad-hoc per includere Sogei nel workflow approvativo di richiesta della password. Tecnicamente, se una persona SAP nominata richiederà l'accesso all'utente *SAPHANADB*, verrà attivato un workflow approvativo e gli utenti dedicati Sogei dovranno approvare questa richiesta;
- Come definito nel *Service Continuity Plan* (Procedura presa in carico SAP CDC da parte di Sogei), Sogei avrà a disposizione due C-User dedicati all'interno della piattaforma SAP per la gestione delle credenziali (CAM); questi due utenti sono anche responsabili di autorizzare l'accesso all'utente tecnico *SAPHANADB* tramite connessione diretta allo strumento CAM. Ciò significa che l'attività che prevede l'utilizzo di *SAPHANADB* potrà essere svolta solo previa approvazione di Sogei;

- Inoltre, Sogei avrà la possibilità di verificare le attività svolte tramite *SAPHANADB* avendo accesso ai log di audit e tecnici al fine di monitorare l'attività SAP;
- Come da richiesta del team Sogei, sarà possibile effettuare il cambio della password di *SAPHANADB* attraverso *service request*. Così come per altre attività standard pianificate/schedulate, il *lead time* e la pianificazione dell'attività di cambio password saranno mutuamente concordati tra Sogei e SAP, tenendo in considerazione del *system downtime* e disponibilità delle risorse da ambo le parti.
- Il *downtime* derivante da tale attività non sarà considerato nel calcolo del livello di servizio.

4.6 SOFTWARE LIFECYCLE INDUSTRIALIZZATO

A completamento del modello, sono richieste le seguenti soluzioni in grado di supportare:

- la gestione delle chiavi di crittografia nello scenario *Bring Your Own Key* (BYOK), attraverso *SAP Data Custodian*, ovvero lo scenario che consente la gestione delle chiavi da parte di Sogei in un HSM o KMS esterno supportato;
- l'evoluzione applicativa ed i processi di trasformazione, valorizzando le funzionalità standard, identificando i colli di bottiglia ed eventuali ottimizzazioni di processo (*SAP Signavio*);
- l'approccio continuo al testing e all'analisi di impatto, al fine di ottimizzare i rilasci in produzione (*SAP Tricentis*).

SAP DATA CUSTODIAN

Prodotto*	Metrica	Quantità
SAP Data Custodian KMS	Connection	40

*La nomenclatura del prodotto potrà essere soggetta a cambiamenti da parte del software vendor

SAP SIGNAVIO

Prodotto*	Metrica	Quantità
SAP Signavio Process Trasformation Manager	User	9
SAP Signavio Process Governance	User	7
SAP Signavio Process Collaboration Hub	User (in blocchi da 10)	10
SAP Signavio Process Modeler	User	9
SAP Signavio Process Governance Collaborator	User (in blocchi da 10)	6
SAP Signavio Process Insights & Intelligence Package	Record (blocchi da 500.000)	3

*La nomenclatura del prodotto potrà essere soggetta a cambiamenti da parte del software vendor

SAP TRICENTIS

Prodotto*	Metrica	Quantità
SAP Change Impact Analysis by Tricentis	Gygabite	5.000

SAP Enterprise Continuous Testing by Tricentis	Connection	15
SAP Enterprise Performance Testing by Tricentis	Object (blocchi da 100)	15

**La nomenclatura del prodotto potrà essere soggetta a cambiamenti da parte del software vendor*

4.7 SAP SAC - SAP Analytics Cloud (post setup)

Di seguito si riporta per la soluzione *SAP Analytics Cloud* l'elenco delle componenti che dovranno essere rese disponibili all'Amministrazione anche nella fase di post setup della SAP CDC. Tali componenti dovranno essere rese disponibili all'Amministrazione fino al 31.12.2026 con possibile interruzione anticipata in caso di dismissione della componente tecnologica:

Prodotto*	Metrica	Quantità
SAP Analyt Cloud, Plan Pred Prof Priv CF	1 Users	200
SAP Analyt Cloud, Plan Pred Std Priv CF	1 Users	4.800
SAP AnlCld HANA upd Pred Priv 512GB CF	256 GB of Memory	1
SAP AnlCld HANA upd Pred Priv 256GB CF	128 GB of Memory	1
SAP AnlCld HANA upd Pred Priv 1024GB CF	512 GB of Memory	1
SAP AnalytCloud test ten pred private CF	1 Users	50
SAP AnalytCloud test ten pred private CF	1 Users	50
SAP AnalytCloud test ten pred private CF	1 Users	50

**La nomenclatura del prodotto potrà essere soggetta a cambiamenti da parte del software vendor.*

4.8 SAP BTP - Business Technology Platform (post setup)

Di seguito si riporta per la soluzione *SAP Business Technology Platform* l'elenco delle componenti che dovranno essere rese disponibili all'Amministrazione anche nella fase di post setup della SAP CDC. Tale componente dovrà essere resa disponibile all'Amministrazione fino alla data di scadenza di SAP CDC:

Prodotto	Metrica	Quantità per anno
Cloud Platform Ent Agrmt, reseller ed	Crediti cloud	1.700.000

Tali crediti cloud sono funzionali all'erogazione dei servizi SAP BTP necessari al funzionamento dell'applicazione ReGis e, più in generale, al supporto delle attività svolte dalla Ragioneria Generale dello Stato nell'ambito di ReGiS.

4.9 Manutenzione On Premise residua

L'introduzione del modello SAP CDC comporterà le seguenti variazioni nella gestione della manutenzione per il parco installato SAP in Sogei. Nel dettaglio, a valle del completamento della fase di setup della SAP CDC, SAP dovrà consentire:

- La terminazione di quelle componenti non in uso presso il parco installato SAP Sogei al momento dell'accensione del servizio SAP CDC;
- Lo spegnimento del costo di manutenzione *on premise*, a completamento del *porting*, per tutte quelle componenti che saranno accolte nel modello SAP CDC.

Di contro, nella fase di post *set-up* e accensione della SAP CDC, Sogei continuerà a sostenere un costo residuo di manutenzione sul modello attuale *on premise* per:

- le componenti software che non confluiscono verso il nuovo modello SAP CDC;
- SAP BusinessObjects per quelle progettualità DAPA e CoGe attualmente non gestite nel Datacenter Sogei;
- Le componenti software SAP IGRUE – ad oggi non in scopo nel percorso di evoluzione verso SAP CDC.

Terminazione delle componenti non in uso nella fase di post setup e accensione della SAP CDC

A valle degli approfondimenti effettuati con i vari team, si riporta di seguito la lista dei prodotti per i quali il diritto d'uso e relativo costo di manutenzione sarà terminato all'attivazione della SAP CDC in quanto non in uso presso l'Amministrazione:

Software non incluso in SAP CDC – SPEGNIMENTO	Qtà
SAP Contract & Lease Mgmt for S/4HANA	1
SAP Enable Now, author option	1
SAP Enable Now, consumption option	1
SAP HANA, active/active, new/subsequent	2
SAP HANA, RT ed Applic & BW-new/subsq	3
SAP Real Estate for S4, retail,ind pr	1
SAP Real Estate Portfolio Mgmt S/4H	1

Spegnimento del costo di manutenzione per le componenti in ambito SAP CDC nella fase di post setup e accensione della SAP CDC

Si riporta di seguito la lista delle componenti che verranno introdotte in ambito SAP CDC e per le quali verrà quindi cessato il costo di manutenzione al momento dell'accensione della SAP CDC.

Software incluso in SAP CDC	Qtà
S/4 Ent. Mgmt. Professional use	40000
S/4HANA EPPM, professional	1
S/4HANA EPPM, standard	1
SAP Access Control for SAP S/4HANA	301
SAP BPC,v f SAP BW/4HANA (BPC), Prof Ed	3988
SAP BPC,v f SAP BW/4HANA (BPC), Std Ed	100

SAP BW/4HANA up to 16 units	5
SAP Disclosure Management, prof. ed.	5
SAP Disclosure Management, standard edit	1
SAP DP by OpenText for SAP S/4HANA	24
SAP DP by OpenText, add-on for BC S/4HANA	24
SAP Ent Proj Connect for SAP S/4HANA	1
SAP HANA, active/active, new/subsequent	6
SAP HANA, RT ed Applic & BW-new/subsq	7
SAP Inv Mgmt by OpenText for SAP S/4HANA	2000
SAP Landscape Management	4
SAP Process Control for SAP S/4HANA	450
SAP Process Orchestration	8
SAP Real Estate for S4, resid pr mgmt opt	1
SAP S/4HANA Fin, cash mgmt (above 1000)	9000
SAP S/4HANA Fin, cash mgmt (first 10)	10
SAP S/4HANA, Developer access	80
SAP, EPPM professional	450
Tax, Benefits & Pay. Proc. for PS for S/4	3
Tax, Benefits & Paym. Proc. for PS for CRM	2
UI data protection logging S/4H	40
UI data protection masking S/4H	40

Per queste componenti Sogei manterrà il diritto d'uso alla licenza sino alla data di rinnovo della SAP CDC. In caso di rinnovo della SAP CDC anche il diritto d'uso nella modalità tradizionale verrà terminato, ovvero, in caso di non rinnovo della SAP CDC, Sogei avrà la possibilità di riattivare le licenze nel modello tradizionale e la relativa manutenzione, previa richiesta entro 30 giorni prima della scadenza del contratto SAP CDC e pagamento del corrispettivo del canone retroattivo a partire dalla data di avvio della SAP CDC.

Manutenzione on premise rimanente nella fase di post setup e accensione della SAP CDC

A conclusione della fase di setup e all'accensione della SAP CDC, Sogei continuerà a sostenere un costo di manutenzione per garantire il supporto alla continuità operativa per quelle componenti che non saranno ricomprese all'interno del nuovo modello SAP CDC.

Software incluso in SAP CDC	Metrica	Qtà	Iniziativa	Qtà
SAP Archiving by OpenText for SAP S/4HANA	Utenti	30.000	INIT / ReGiS	La gestione dei documenti di INIT e ReGiS a tendere potrà essere effettuata dalla piattaforma centrale <i>Documentum</i> . Nel periodo transitorio l'attuale documentale <i>OT Archive Center</i> continuerà ad essere integrato con i sistemi in SAP CDC
SAP Business Planning and Consolidation, version for Microsoft	Utenti	15	Consolidato PA	BPC 10 for Microsoft, configurato per la gestione del report di consolidamento della PA.

<i>Platform, professional edition</i>				
SAP <i>Business Planning and Consolidation, version for Microsoft Platform, standard edition</i>	Utenti	85	Consolidato PA	BPC 10 for Microsoft, configurato per la gestione del report di consolidamento della PA.
<i>S/4 Enterprise Mgmt. for Functional use</i>	Utenti	1	INIT /ReGiS	
SAP <i>BusinessObjects Enterprise (CS)</i>	CS	33	Cross	Set di licenze necessarie per le installazioni SAP BO non incluse nella SAP CDC (Progetto DAPA e CoGe)
SAP <i>BusObj Enterprise Premium (CPU)</i>	CPU	3	Cross	Set di licenze necessarie per le installazioni SAP BO non incluse nella SAP CDC (Progetto DAPA e CoGe)
SAP <i>BusObj Web Intelligence (CPU)</i>	CPU	2	Cross	Set di licenze necessarie per le installazioni SAP BO non incluse nella SAP CDC (Progetto DAPA e CoGe)

4.10 Altri requisiti della fornitura

4.10.1 Certificazioni della soluzione CDC

Le componenti oggetto del presente documento dovranno essere erogate nel rispetto delle certificazioni richieste per la soluzione SAP CDC:

- ISO 27001 - *Information Security Management System*;
- ISO 27017 - *Implementation of cloud specific information security controls*;
- ISO 27018 - *Protection of personal data in the cloud*;
- ISO 22301 - *Business Continuity Management Systems*.

4.10.2 Qualifica ACN

I servizi cloud oggetto di acquisizione, in particolare con riferimento alle soluzioni SAP BTP – SAP *Business Technology Platform* e SAP SAC – SAP *Analytics Cloud*, dovranno essere qualificati, per **i dati ordinari**, ai sensi del decreto direttoriale n. 21007 del 27 giugno 2024 dell'Agenzia nazionale per la Cybersicurezza. Il requisito dovrà essere posseduto ai fini della stipula e per tutta la fase esecutiva, secondo la disciplina contenuta nel Contratto.

4.10.3 Cybersicurezza - DPCM del 15 giugno 2021

La presente acquisizione ricade nel perimetro di sicurezza nazionale cibernetica, ai sensi di quanto previsto al D.L. 105/2019 convertito in l. 133/2019 e relativi decreti attuativi, in quanto nell'oggetto dell'appalto sono inclusi uno o più beni, sistemi o servizi ICT destinati ad essere impiegati nel perimetro della sicurezza nazionale cibernetica, tra quelli individuati dal **DPCM del 15 giugno 2021**, pubblicato in data 19/08/2021.

Sogei, in conformità a quanto previsto dall'art. 5 del d.p.r. 54/201, ha provveduto a richiedere apposito parere al CVCN (prot. 0002370 Reg. U. del 30 luglio 2025, AOO_ACN – KS/S300/5.1.12) che ha stabilito le misure di sicurezza da adottare e i test da eseguire.

Dal momento che la soluzione, costituente nel suo complesso il cosiddetto "*Oggetto della Fornitura*" (OdF), risulta, in effetti, composta da diverse tecnologie, alcune delle quali riconducibili alle categorie di cui al DPCM 15 giugno 2021, tra cui componenti di rete come router, switch e bilanciatori di carico, sono richiesti, in esito alle verifiche preliminari e considerate le condizioni di impiego dell'OdF (Oggetto di fornitura), ai sensi dell'art. 4, comma 3 e dell'art 5, comma 3, del DPR 5 febbraio 2021, n. 54, l'esecuzione di test con **severità ALTA** per la:

- verifica della corretta implementazione delle funzionalità di sicurezza;
- verifica di intrusione, a supporto dell'analisi di vulnerabilità.

Il fornitore è tenuto a:

- a) assicurare la propria collaborazione con la Committente e con il Centro di Valutazione e Certificazione Nazionale (CVCN), per l'allestimento di un ambiente di test, adeguatamente rappresentativo della realtà di esercizio dell'oggetto di fornitura, ovvero in grado di replicare un contesto operativo che consenta di analizzare la corretta
- b) mettere a disposizione del CVCN le evidenze di cui all'art. 5, comma 5, lettere a), c), d) ed e) del DPR 5 febbraio 2021, n. 54, di cui, nel seguito, si forniscono le informazioni generali e i requisiti di dettaglio. Si ricorda che l'avvio dei test è subordinato alla ricezione di dette evidenze con i contenuti attesi e, pertanto, quanto prima esse saranno rese disponibili tanto più rapidamente potrà concludersi l'iter amministrativo;
- c) garantire, per tutta la durata del contratto, servizi di supporto che includano il rilascio degli aggiornamenti di sicurezza.

Dovranno essere applicate le misure di sicurezza di cui al DPCM 14 aprile 2021 n. 81.

Tenuto conto della natura composita dell'OdF, gli specifici apparati da sottoporre a test e il dettaglio delle attività di valutazione da eseguire potranno essere individuati solo all'esito dell'aggiudicazione/stipula del contratto, allorquando Sogei dovrà comunicare, ai sensi dell'art. 5 comma 9 del D.P.R. 5 febbraio 2021, n. 54, l'elenco puntuale di tutte le componenti afferenti alle citate categorie del DPCM 15 giugno 2021 incluse nella piattaforma SAP-CDC, identificandone in modo univoco modello e versione del *firmware*, oltre a indicare il fornitore contraente.

Nella fase di preparazione dei test che consegnerà alla predetta comunicazione, il CVCN potrà meglio indirizzare, nei rapporti diretti con il fornitore, la richiesta della specifica documentazione, genericamente indicata al precedente punto b), relativa a ciascuna componente individuata, funzionale all'esecuzione dei test.

La Tabella seguente riporta le attività propedeutiche, previste dal DPR 54/2021, di cui all'art.5 comma 5, che il Fornitore è tenuto ad effettuare in caso di imposizione di test da parte del CVCN. Tali attività sono indispensabili ai fini dell'esecuzione dei test e devono concludersi nella fase di preparazione (Art. 6 del DPR 54/2021) come condizione necessaria per il proseguimento alla fase di attuazione.

Art.5, comma 5	a)	fornire evidenza dell'idoneità delle funzionalità di sicurezza e delle loro configurazioni a soddisfare i requisiti di sicurezza definiti nel documento di Analisi del Rischio;	[1]
	b)	provvedere all'allestimento di un ambiente di test adeguatamente rappresentativo della realtà di esercizio presso il laboratorio o, se necessario, presso il Fornitore o presso il Soggetto del perimetro;	[2]
	c)	fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzionalità;	[3]
	d)	fornire una descrizione delle funzionalità di sicurezza implementate nell'oggetto di valutazione;	[4]
	e)	fornire una descrizione dei test funzionali e di sicurezza già eseguiti dal Fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.	[5]

Le evidenze di dettaglio, da intendersi come un approfondimento degli elementi in Tabella, sono necessarie al CVCN per applicare la metodologia interna di test (riservata) e sono elencate di seguito, in termini di singoli documenti. Ciascun documento, o sua parte, è tracciato verso gli elementi di maggiore astrazione riportati in Tabella.

La ricezione di tutti i documenti, con i requisiti di contenuto specificati contestualmente, presupposto per la conclusione della fase di preparazione e l'avvio della fase esecutiva che si concluderà entro i termini di 60 gg individuati come all'Art. 4 comma 5 del citato DPR.

Per l'avvio della fase esecutiva dei test è necessaria anche la corretta conclusione di quanto previsto al punto [2] della Tabella. In particolare, il Fornitore, al meglio delle sue possibilità e con il supporto della Committente ed eventualmente del produttore, deve mettere a disposizione:

- l'Oggetto della Fornitura (OdF) completo, che sia:
- configurato in modo adeguato a eseguire le verifiche (con il supporto della Committente, l'OdF deve venire configurato in modo da rappresentare la realtà di esercizio, ossia con le funzioni di sicurezza e le caratteristiche, conformemente all'Analisi dei Rischi, considerate e descritte nella comunicazione effettuata al CVCN per intenzione di acquisto, ai sensi dell'art. 1, comma 6, lettera a) del D.L. 21 settembre 2019 n. 105);

- corredato del riferimento univoco dell'OdF, ossia: identificazione univoca dell'OdF, o dei prodotti che compongono l'OdF, con indicazione della versione del software/firmware.

L'ambiente di test, il cui allestimento è previsto a cura del Fornitore, dovrà essere preparato su piattaforma fisica o virtuale preferibilmente presso i laboratori del CVCN, oppure, qualora necessario e previa richiesta motivata per iscritto, presso le strutture del Committente o presso le strutture del Fornitore. Si veda, a tal proposito, il DPR del 5 febbraio 2021, n. 54 art. 5 comma 5 lettera b) e, specificamente per quanto riguarda la sede delle attività, l'art. 6 comma 4 lettera b).

Sono inoltre richieste le immagini del software/*firmware* dell'OdF, o delle sue componenti, ove disponibili, accompagnate dalla relativa documentazione tecnica (che ne specifichi, tra gli altri dettagli, il numero esatto della versione). È anche attesa la disponibilità da parte del Fornitore, laddove possibile, a rendere disponibile il firmware per esecuzione in ambiente virtuale.

Di seguito sono indicati, specificando i requisiti generali di contenuto, alcuni documenti che è necessario fornire al CVCN e che sono condizione necessaria per avviare la fase di test. I documenti sono attesi a cura del Fornitore che tuttavia, in taluni casi, potrà avvalersi del supporto del Committente o del supporto da parte dello sviluppatore/produttore dell'OdF.

La versione più aggiornata della documentazione tecnica dell'Oggetto della Fornitura (OdF), ovvero il datasheet e, ove presente, il *reference manual* e/o *technical manual* per sviluppatori possono essere utili per reperire, almeno in parte, le informazioni elencate di seguito.

In caso di pregressa certificazione *Common Criteria* (ISO/IEC 15408) conseguita dall' OdF o sue componenti (nella esatta versione e configurazione di fornitura), i requisiti seguenti possono essere soddisfatti (in tutto o in parte, secondo indicazione del CVCN fornita caso per caso) inoltrando l'intero pacchetto documentale valutato dal laboratorio ITSEF2 nel contesto di detta certificazione di sicurezza.

[CST] - Custom Security Target

Il Committente/Fornitore (C/F) deve mettere a disposizione un documento (anche detto "Custom" Security Target) contenente le seguenti informazioni

1. (F) vista grafica dell'architettura ad alto livello del prodotto/sistema [3];
2. (F) la descrizione della modalità d'uso dell'OdF [3];
3. (F) la descrizione ad alto livello delle funzionalità di sicurezza offerte dall'OdF [3], [4];
4. (F) l'indicazione della categoria generale (N.B. non correlata ad una delle categorie individuate nel DPCM 15/06/2021) di appartenenza dell'OdF e delle componenti di terze parti necessarie per la corretta operatività dell'OdF [3];

5. (F) la descrizione dettagliata delle funzionalità di sicurezza dell'OdF, compresa la lista di hardware, software e firmware nell'ambiente di esercizio, necessari per il funzionamento dell'OdF [3],[4];
6. (F) l'ambito di applicazione fisico (lista di hardware, software e firmware) e logico (lista di componenti logiche) dell'OdF [3], [4];
7. (F) la descrizione degli obiettivi di sicurezza per l'ambiente in cui opera l'OdF (da intendersi come ipotesi sull'ambiente operativo, nella forma di misure di sicurezza tecnica, procedurale, di natura fisica o relativa al personale, che deve essere rispettata affinché l'OdF possa operare correttamente) [1], [2];
8. (C) la descrizione delle funzionalità di sicurezza dell'OdF in relazione ai requisiti di sicurezza derivanti dall'Analisi dei Rischi (c.d. TOE Summary Specification secondo la terminologia ISO/IEC 15408 Common Criteria) e la dimostrazione che siano appropriate per i requisiti di sicurezza identificati [1], [3], [4];

[OUG] – Manuale Operativo per l'utente

Il Fornitore deve mettere a disposizione il manuale operativo (*operational user guidance*) per l'utente (focalizzato agli aspetti di sicurezza [2], [3] contenente:

1. la definizione dei ruoli degli utenti;
2. per ogni ruolo:
 - a. le funzionalità accessibili;
 - b. i privilegi associati;
 - c. eventuali segnalazioni nella forma di "*Warnings*" di sicurezza relativamente all'uso di funzionalità e privilegi associati ai ruoli;
 - d. indicazioni per l'utilizzo sicuro delle interfacce dell'OdF;
 - e. le funzionalità di sicurezza e le interfacce a disposizione con l'indicazione di tutti i parametri previsti dall'interfaccia, compresi i valori che garantiscono l'uso sicuro dell'interfaccia stessa e dell'OdF;
 - f. la descrizione delle conseguenze di ogni evento di sicurezza rilevante a seguito dell'uso delle funzionalità accessibili ad ogni utente (per ogni ruolo utente) e le modalità con il quale esso può intervenire per garantire/ristabilire l'uso in sicurezza;
 - g. la descrizione di tutti i possibili modi di utilizzo dell'OdF al fine di garantire il mantenimento dello stato sicuro dell'OdF;
 - h. la descrizione, per ogni ruolo utente, di quali misure di sicurezza seguire (ovvero procedure applicare) in modo tale da soddisfare gli obiettivi di sicurezza per l'ambiente operativo;

[SETUP] - Descrizione delle procedure di predisposizione e messa in esercizio

dell'OdF

Il Fornitore deve mettere a disposizione un documento con la descrizione delle procedure di predisposizione e messa in esercizio dell'OdF [2], [3] contenente:

1. la descrizione di tutte le operazioni necessarie per l'installazione sicura dell'OdF;
2. la descrizione di tutte le operazioni necessarie per la preparazione sicura dell'ambiente operativo nel rispetto dei requisiti di sicurezza;
3. la descrizione relativa alle componenti coinvolte e alle modalità impiegate per garantire l'avvio sicuro ("*secure boot*") e l'aggiornamento del software sicuro ("*secure update*");
4. la descrizione della configurazione effettiva e completa effettuata dal Fornitore per lo specifico caso d'uso; corredata dalla sua relativa documentazione tecnica, eventualmente mascherando i parametri sensibili ivi contenuti.

[FSP] - Descrizione delle specifiche funzionali di sicurezza

Il Fornitore deve mettere a disposizione un documento con la descrizione delle specifiche funzionali di sicurezza [4] contenente, in particolare:

1. una rappresentazione completa delle funzionalità di sicurezza dell' OdF;
2. la descrizione dello scopo e delle modalità di uso delle interfacce che forniscono funzionalità di sicurezza dell'OdF (di seguito interfacce di sicurezza dell'OdF);
3. la descrizione di tutti i parametri associati ad ogni interfaccia di sicurezza dell'OdF;
4. la descrizione di tutte le azioni associate alle interfacce di sicurezza;
5. la descrizione di tutti i messaggi di errore che possono essere generati a seguito della stimolazione delle interfacce di sicurezza;
6. la mappatura tra le interfacce e le funzionalità di sicurezza dell'OdF.

[TEST] - Documentazione relativa ai test già effettuati

Il Fornitore deve mettere a disposizione la documentazione relativa ai test già effettuati dal produttore che mostri la corrispondenza tra i test eseguiti e le interfacce di sicurezza riportate nella descrizione delle specifiche funzionali di sicurezza [5].

La documentazione di test deve contenere:

1. i piani di test effettuati (indicano i test che sono stati eseguiti e la descrizione dello scenario di esecuzione, indicando anche le eventuali dipendenze dai risultati di altri test);
2. risultati attesi e i valori effettivamente ottenuti;

3. l'analisi con matrice di copertura che indichi la corrispondenza tra:
 - a. i test eseguiti e
 - b. Le interfacce delle funzionalità di sicurezza, riportate nella descrizione delle specifiche funzionali di sicurezza, in modo da produrre evidenza che tutte le interfacce delle funzionalità di sicurezza siano state sottoposte a test [5];

[DEPTH] - Documentazione relativa ai test già effettuati (se disponibile)

Il Fornitore deve mettere a disposizione un documento con l'analisi della profondità dei test (*analysis of the depth of testing*, [5]), predisposta in modo da:

1. dimostrare la corrispondenza tra i test, nella documentazione dei test effettuati, e i sottosistemi, ed eventualmente i moduli, che implementano le funzionalità di sicurezza;
2. dimostrare che tutti i sottosistemi, ed eventualmente tutti i moduli, che implementano le funzionalità di sicurezza siano stati sottoposti a test;

[DESIGN] - Descrizione dell'architettura

Il Fornitore deve mettere a disposizione un documento con l'architettura costitutiva dell'OdF (c.d. TOE design secondo la terminologia ISO/IEC 15408 Common Criteria) [3] contenente, in particolare:

1. descrizione della struttura dell'OdF in termini di sottosistemi ed eventualmente moduli;
2. identificazione e descrizione di tutti i sottosistemi interessati dalle funzionalità di sicurezza dell'OdF e relative modalità di interazione;
3. mappatura di ciascun sottosistema ed eventualmente modulo sulle interfacce alle funzionalità, di sicurezza;
4. eventuale descrizione di ogni modulo che implementa le funzionalità di sicurezza (*SFR-enforcing*) in termini di obiettivi e relazioni con altri moduli;
5. eventuale descrizione di ogni modulo che implementa le funzionalità di sicurezza (*SFR-enforcing*) in termini di interfacce relative alle funzionalità di sicurezza (*SFR-related*), valori in output delle interfacce, interazioni con altri moduli e interfacce relative alle funzionalità di sicurezza (*SFR-related*) rispetto ai moduli che implementano le funzionalità di sicurezza (*SFR-enforcing*);
6. eventuale descrizione di ogni modulo, da cui dipendono (*SFR-supporting*) e non dipendono (*SFR non-interfering*) le funzionalità di sicurezza, in termini di obiettivi e relazioni con altri moduli.

[TOOLS] - Strumenti specialistici (se necessari)

Il Fornitore deve mettere a disposizione un insieme di risorse (a titolo di esempio strumenti specialistici utilizzati per fare i test, ecc.) equivalente a quelle che sono state necessarie al fornitore per svolgere i test delle funzionalità di sicurezza dell'OdF [2];

[IMPL] - Rappresentazione dettagliata dell'implementazione dell'OdF (Se disponibile)

Il Fornitore (con il supporto dello sviluppatore/produttore se non coincidente) deve mettere a disposizione, secondo quando richiesto dal CVCN ai fini dell'esecuzione dei test, una rappresentazione dettagliata dell'implementazione dell'OdF (ad esempio: codice sorgente, componenti di sviluppo, diagrammi UML) in modo tale che l'OdF possa essere riprodotto in modo esatto, inequivocabile e completo, e sia possibile confermare la corrispondenza tra progettazione dell' OdF e un campione generato a partire dalla rappresentazione fornita [2];

[DEVI] - Descrizione degli strumenti di sviluppo

Il Fornitore (con il supporto dello sviluppatore/produttore se non coincidente) deve mettere a disposizione un documento che descriva gli strumenti utilizzati per lo sviluppo sicuro dell'OdF [4] (development tool).

4.10.4 Cybersicurezza - DPCM del 30 Aprile 2025

Trovano applicazione le previsioni di cui al DPCM del 30 aprile 2025, per cui essendo l'iniziativa finalizzata alla tutela di interessi nazionali strategici ed avendo la stessa ad oggetto, tra l'altro, anche servizi che rientrano tra le categorie indicate nell'All. 2 del predetto decreto, gli elementi essenziali di cui all'All. 1 del medesimo decreto sono da considerarsi quali requisiti minimi della fornitura.

Sogei si riserva, in fase esecutiva, di effettuare controlli in merito all'effettivo rispetto degli stessi (cioè requisiti/elementi essenziali), pena la risoluzione del Contratto.

4.11 Pianificazione dell'attività di moving

La *roadmap* evolutiva delle soluzioni SAP è stata definita per consentire a Sogei di raggiungere i seguenti obiettivi:

- Accelerare l'adozione del SAP CDC ed il contestuale spegnimento della manutenzione attuale;
- Realizzare la separazione tra INIT e ReGiS per le piattaforme *S/4HANA* e *BW/4HANA*;
- Ottimizzare le attività di aggiornamento delle soluzioni *S/4HANA* e *BW/4HANA* verso l'ultima versione rilasciata da SAP, accelerando il processo di trasformazione digitale;
- Sincronizzare le attività di *move to SAP CDC* con gli obiettivi di business non impattando quindi i principali rilasci già pianificati;
- Supportare l'evoluzione del sistema Finanziario SAP IGRUE, accelerando l'avvio dell'iniziativa all'interno della piattaforma ReGiS;

- Minimizzare e mitigare i rischi progettuali.

L'approccio operativo al *move* delle applicazioni nel modello SAP CDC dovrà tenere conto delle seguenti assunzioni:

- La fase di preparazione richiede la disponibilità dei team Sogei, SAP e dei *System Integrator* sulle diverse aree coinvolte;
- Accensione del servizio SAP CDC progressivo a partire da 6 mesi dalla firma del contratto;
- Approccio alla migrazione differenziato per cluster di sistema: *S/4HANA*, *BW/4HANA*, *SAP BO*, altre soluzioni SAP;
- Per i sistemi BO, considerando il consolidamento applicativo previsto, si prevede un approccio progressivo di *move* su SAP CDC che dovrà terminarsi entro 12 mesi dalla stipula contrattuale;
- In generale, i sistemi oggetto di *move* dovranno essere in una versione compatibile con la SAP CDC.

Nel *move* delle applicazioni in SAP CDC, SAP definirà nel dettaglio modalità ed attività tecniche di migrazione. Nello specifico SAP si farà carico di eseguire servizi specialistici per:

- Analizzare e censire le modalità di accesso e le integrazioni attuali;
- Definire il piano di migrazione/aggiornamento ed il dettaglio degli step tecnologici e la verifica dei prerequisiti;
- Coordinare e supportare l'installazione delle componenti SAP CDC e, ove previsto, le attività di aggiornamento e configurazione delle soluzioni SAP;
- Definire le attività di *networking* all'interno della *subnet* SAP CDC coerentemente con le indicazioni del cliente
- Garantire a Sogei il completamento del *move* verso SAP CDC. In particolare, di seguito si riportano le macro-aree che saranno gestite da SAP per garantire il buon esito del *move*:
 - attività tecniche di aggiornamento delle soluzioni SAP (ove previsto);
 - attività tecniche di migrazione e post-migrazione;
 - validazione delle integrazioni attraverso test unitari con i sistemi afferenti alla SAP CDC.

È richiesto il supporto del team Sogei per:

- Coordinamento delle strutture coinvolte lato Sogei (*network*, Infrastruttura, etc.) per garantire i prerequisiti necessari all'aggiornamento delle soluzioni SAP per la migrazione su SAP CDC;
- Accesso ai sistemi attuali;
- Chiusura dei sistemi attuali durante le attività di *cut-over*;
- Integrazioni tool terze parti (Es. SSO)

- Configurazione lato Sogei degli aspetti di networking prima del *demarcation point* della SAP CDC (DNS, *firewall*, definizione hostname) e firma certificati se richiesti;
- Adeguamento delle applicazioni e/o programmi custom per garantire che il funzionamento iso-funzionale della soluzione anche sulle personalizzazioni;
- Esecuzione dei test di non regressione della parte applicativa.

I sistemi in ambito del progetto di migrazione verso la SAP CDC sono di seguito dettagliati:

Landscape	#Sistemi	Versione	CDC Readiness	Approccio Adozione SAP CDC
SAP S/4HANA – INIT	8	S/4HANA 1909	Supportato tramite attivazione <i>Safekeeper</i>	<i>Move</i> contestuale/ <i>Split</i> * + successivo Upgrade
SAP S/4HANA – ReGiS	8	S/4HANA 1909	Supportato tramite attivazione <i>Safekeeper</i>	<i>Move</i> contestuale/ <i>Split</i> * + successivo Upgrade
SAP S/4HANA – Play	1	S/4HANA 1909	Supportato tramite attivazione <i>Safekeeper</i>	<i>Move</i> (creato come system copy)
SAP BW/4HANA – INIT	8	BW/4HANA 2.0	Necessario upgrade <i>OnPremise</i>	<i>Move/Split</i>
SAP BW/4HANA – ReGiS	4	BW/4HANA 2.0	Necessario upgrade <i>OnPremise</i>	<i>Move/Split</i>
SAP PO	4	SAP NetWeaver 7.5	Versione supportata	<i>Move</i>
SAP GRC Process	3	SAP NetWeaver ABAP 7.52	Versione supportata	<i>Move</i>
Adobe Document Service	4	SAP NetWeaver 7.5	Versione supportata	<i>Move</i>
<i>Solution Manager</i>	2	SAP Solution Manager 7.2	Versione supportata	<i>Move</i>
SAP Business Object – INIT	6	SBOP BI PLATFORM 4.3	Versione supportata	Approccio <i>greenfield</i> con migrazione applicativa
SAP Business Object – ReGiS	4	SBOP BI PLATFORM 4.3	Versione supportata	Approccio <i>greenfield</i> con migrazione applicativa
SAP Business Object – Area RGS	5	SBOP BI PLATFORM 4.3	Versione supportata	Approccio <i>greenfield</i> con migrazione applicativa
SAP Business Object – Tessera Sanitaria	3	SBOP BI PLATFORM 4.3	Versione supportata	Approccio <i>greenfield</i> con migrazione applicativa
SAP Business Object – DWHRGS	5	SBOP BI PLATFORM 4.2	Versione NON supportata, approccio <i>greenfield</i> su SAP BO 4.3	Approccio <i>greenfield</i> con migrazione applicativa
SAP Business Object – BDAP	5	SBOP BI PLATFORM 4.2	Versione NON supportata, approccio <i>greenfield</i> su SAP BO 4.3	Approccio <i>greenfield</i> con migrazione applicativa

* Il dettaglio dell'approccio progettuale sul singolo ambiente è descritto nel seguito

Si specifica che:

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

- L'ambiente di "Play" sarà utilizzabile sia per INIT che per ReGiS;
- I sistemi SAP S/4HANA di INIT e ReGiS saranno aggiornati all'ultima release disponibile dopo aver ultimato la migrazione su SAP CDC;
- L'aggiornamento del sistema SAP BW/4HANA dovrà avvenire nell'attuale infrastruttura (*OnPremise*), successivamente sarà possibile effettuare il *move* su SAP CDC;
- SAP S/4HANA – ReGiS è stato dimensionato per ospitare anche in futuro le funzionalità del Sistema SAP IGRUE.

In particolare, lo *shift* applicativo su SAP CDC è articolato due fasi:

- **FASE DI PREPARAZIONE** - raggruppa tutte le attività preliminari di definizione:
 - di un piano integrato di dettaglio per il *move*,
 - della strategia di aggiornamento e test delle soluzioni in ambito;
 - progettazione tecnica (censimento, integrazioni, *network*, etc.);
 - supporto per il *change management* per l'adeguamento del modello di *technical operation* a fronte dell'adozione di SAP CDC.
- **FASE DI ESECUZIONE** – raggruppa tutte le attività di conduzione del *move* dei sistemi su SAP CDC, in generale si prevedono i seguenti task:
 - Definizione piano di *Cut-over*;
 - Esecuzione attività di *move* dei sistemi su SAP CDC con attività tecniche di post-migrazione;
 - Esecuzione attività di test e validazione delle integrazioni;
 - Rilascio dei sistemi;
 - Supporto *post-go-live*.

4.11.1 PREPARAZIONE – ATTIVITÀ PRELIMINARI ALL'ATTIVAZIONE SAP CDC

Con l'obiettivo di definire una visione complessiva architetturale e mitigare i rischi progettuali, si riportano di seguito le macro-attività preparatorie all'esecuzione del *move* sulla SAP CDC.

L'esecuzione di tali attività, oltre ad indirizzare i temi specifici di ciascuno stream, consentirà di sviluppare e definire una pianificazione integrata e condivisa tra tutti i gruppi coinvolti.

- **Stream 1. Preparazione provisioning CDC / Move to CDC dei sistemi in ambito**

I macro-task prevedono:

- La predisposizione di un piano di lavoro integrato.
- L'ispezione dei datacenter per verificare la compatibilità dei server, il loro posizionamento e la distanza dagli apparati di rete.
- Il disegno dell'integrazione di rete e l'identificazione della posizione fisica all'interno dei datacenter.
- La predisposizione dei cablaggi di rete e alimentazione elettrica.
- L'identificazione dei requisiti di separazione tra INIT-ReGIS S/4 e BO, come la riconfigurazione funzionale e l'OAM.
- L'assessment della configurazione dei meccanismi di *Single Sign-On (SSO)*.

- Il mapping delle interfacce e dei sistemi coinvolti, con la progettazione dei test di connettività.
- L'identificazione delle regole *firewall* da attivare o disattivare lato Sogei.
- Il disegno dell'architettura logica del *frontend*.
- La definizione e predisposizione del monitoraggio dell'infrastruttura, integrato con la *Control Room*.

I Team coinvolti in questa fase sono: Sogei Rete; Sogei OAM (Oracle); Sogei Basis; Sogei Architetture; Sogei Applicativi INIT/ReGIS; Sogei *Control Room*; Team *System Integrator*; Team SAP Servizi; Team SAP CDC (ECS).

- **Stream 2 - Focus Operation / Conduzione**

I macro-task prevedono:

- La gestione del *change management* operativo per SAP CDC.
- L'individuazione dei processi core.
- La definizione della strategia di test e del piano di test per l'ottimizzazione del testing tramite Tricentis.
- L'identificazione degli scenari applicativi critici per l'attivazione del monitoraggio avanzato.
- L'avvio del progetto per l'attivazione di ChaRM.
- La gestione delle utenze *Firefighter*.

I Team coinvolti in questa fase sono: Sogei Basis; Sogei Applicativi INIT/ReGIS; Team *System Integrator*; Team SAP Servizi; Team SAP CDC (ECS).

- **Stream 3 – Focus predisposizione Upgrade S/4HANA**

I macro-task prevedono:

- Analisi impatto ed evoluzioni correlate alla nuova release S/4HANA (*Readiness Check – Custom Code Analysis*)
- Preparazione Piano Lavoro di dettaglio evoluzione dei sistemi SAP e coinvolgimento degli stakeholders
- Verifica matrice di compatibilità sistemi afferenti
- Definizione dei casi di test
- Predisposizione SAP *Signavio* supporto analisi processi per aggiornamento sistema.

I Team coinvolti in questa fase sono: Sogei Basis; Sogei Applicativi INIT/ReGIS; Team *System Integrator*; Team SAP Servizi; Team SAP CDC (ECS).

- **Stream 4 – Focus aggiornamento Release BW/4HANA**

I macro-task prevedono:

- Requisiti, strategia per aggiornamento BW/4HANA
- Analisi impatto ed evoluzioni correlate alla nuova release BW/4HANA
- Aggiornamento BW/4HANA in infrastruttura on premise
- Definizione dei casi di test
- Esecuzione Upgrade su tutti gli ambienti in scope

I Team coinvolti in questa fase sono: Sogei Basis; Sogei Applicativi INIT/ReGIS; Team *System Integrator*; Team SAP Servizi; Team SAP CDC (ECS).

4.11.2 ESECUZIONE – ATTIVITÀ PER LA MIGRAZIONE DELLE PIATTAFORME IN SAP CDC

L'approccio alla migrazione è stato differenziato a seconda della tipologia di sistema e delle necessità. A prescindere dalle specificità dell'approccio, dovranno essere previste le attività a conferma del buon esito della migrazione:

- Attività tecniche di post-migrazione
- Attività di test e validazione delle integrazioni
- Rilascio dei sistemi

Tutte le attività saranno corredate da uno studio preliminare delle configurazioni attuali, da procedure di *Dry Run* prima della messa in onda degli ambienti produttivi e da piano di *cut-over*.

Si riporta di seguito l'ipotesi di piano di massima suggerito per le attività di shift verso la SAP CDC:

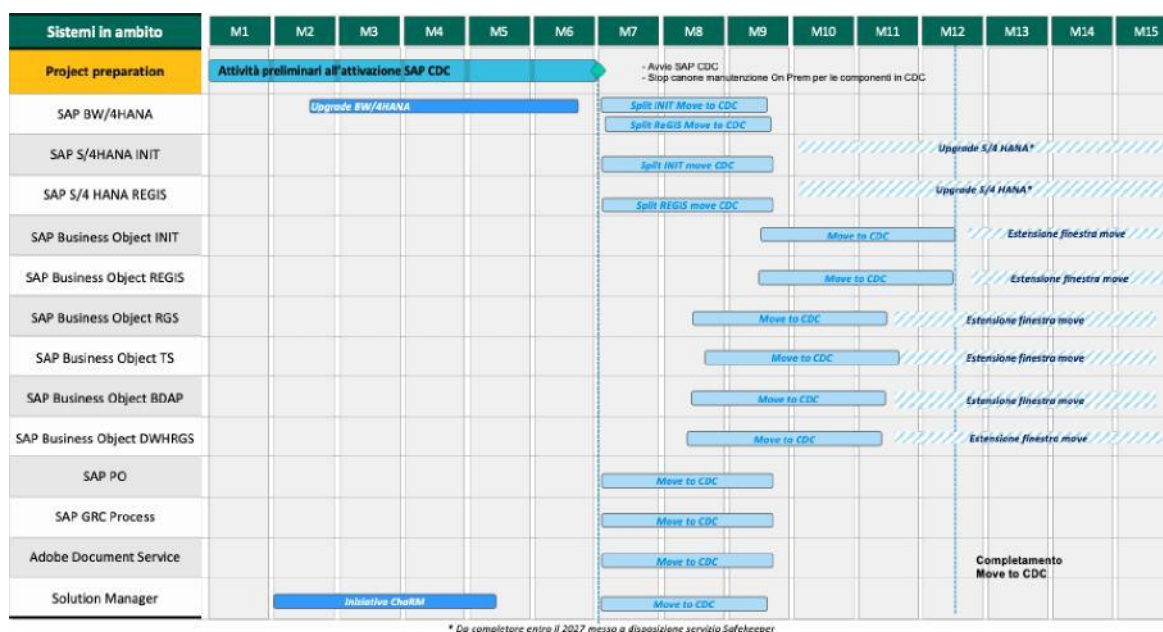


Figura 15 - Ipotesi di piano per la migrazione verso SAP CDC

L'approccio ed il timing della pianificazione delle attività saranno perfezionati dal gruppo di lavoro esteso tecnico/applicativo, congiuntamente con il team SAP, in modo da ottimizzare le attività e minimizzare gli impatti di business.

Si riporta nei seguenti paragrafi le descrizioni preliminari dell'approccio alla migrazione per ciascuna tipologia di *cluster*.

4.11.2.1 S/4HANA MOVE E SPLIT CONTESTUALE

Il servizio SAP *Safekeeper* consente l'estensione della finestra di gestione dei sistemi SAP S/4HANA su SAP CDC a fine del ciclo di manutenzione. Attualmente le installazioni SAP S/4HANA per i programmi INIT e Regis sono in versione 1909, versione non supportata in SAP CDC.

L'approccio per i sistemi SAP S/4HANA prevederà la separazione (*split*) delle progettualità INIT e ReGis contestuale alla procedura di *move* su SAP CDC.

In particolare, si procederà con la separazione degli ambienti INIT e ReGis su nuove istanze attraverso i seguenti passi:

- Backup dell'attuale sistema SAP S/4HANA
- Restore del backup in SAP CDC su due ambienti distinti dedicati rispettivamente a INIT e ReGis
- Riconfigurazione delle connessioni con stesso alias per i rispettivi ambienti INIT e ambiente ReGis
- Rilascio sistemi
- Pulizia mandanti non utilizzati sui rispettivi ambienti
- Creazione mandante per progettualità IGRUE (se richiesto) su ambiente ReGis

L'aggiornamento di release per la parte tecnica di SAP S/4HANA potrà essere pianificato ed eseguito successivamente al *move* su SAP CDC attraverso il supporto del team SAP ECS entro il 31.12.2027.

4.11.2.2 BW/4HANA UPGRADE on Premise

L'adeguamento della release in matrice di compatibilità con SAP CDC dovrà essere eseguito sugli ambienti *on Premise* per la soluzione SAP BW/4HANA dal team SAP, successivamente viene eseguita l'attività di *move* su SAP CDC come specificato di seguito.

- MOVE

L'approccio per il *move* utilizzata per i sistemi SAP BW/4HANA prevederà i seguenti step:

- Backup dell'attuale sistema
- Esecuzione *restore* su ambienti SAP CDC
- Riabilitazione delle connessioni con stesso alias ambienti on premise
- Rilascio sistema

- SPLIT

Completato il *move* di SAP BW/4HANA su CDC sarà eseguita la separazione fisica con i seguenti step:

- Backup dell'attuale sistema
- Esecuzione *restore* su ambienti BW/4HANA dedicato in SAP CDC per Regis
- Riabilitazione delle connessioni con stesso alias ambienti *on premise*
- Rilascio sistema.

La pulizia dei dati INIT sul nuovo ambiente BW/4HANA dedicato a Regis sarà di tipo applicativo eseguita dai *System integrator* con il supporto del team SAP.

La separazione delle applicazioni INIT e Regis per la componente SAP BPC e SAP BW può essere valutata con altri approcci per ottimizzare la fase di *Upgrade* e la finestra di *down-time*.

4.11.2.3 APPROCCIO GREENFIELD CON MIGRAZIONE APPLICATIVA SAP BO

L'approccio al *move*, specifico per le componenti SAP BO, è di tipo *Greenfield* ed è costituito dai seguenti macro-passi:

- Installazione ambiente SAP BO (versione 4.3, ultimo SP disponibile) su infrastruttura SAP CDC e migrazione configurazione tecnica comprendente l'*export* e la *content promotion* - attività eseguita dal team SAP per la migrazione
- Migrazione applicativo/funzionale degli oggetti SAP BO eseguita dal team funzionale Sogei con il supporto del team di migrazione SAP.

L'installazione sarà eseguita su database SAP ASE all'ultimo livello di *support package* e saranno migrate tutte le configurazioni tecniche dell'attuale sistema, in termini di autenticazione e *repository* tecnico.

In merito ai due *landscape* addizionali di *BusinessObjects DWHRGS* e *BDAP*, considerando che è necessario una rivisitazione delle configurazioni (es. *OAM*, *repository*, etc.), per questi sistemi si prevede una nuova installazione con configurazione dei *landscape* secondo i nuovi requisiti. Tale attività sarà effettuata nell'ambito dei servizi specialistici SAP.

4.11.2.4 MOVE ALTRI SISTEMI SAP

L'approccio al *move* utilizzato per tutti i sistemi che non necessitano aggiornamento tecnologico dovrà prevedere i seguenti step:

- *Backup* dell'attuale sistema
- Esecuzione *restore* su ambienti SAP CDC
- Riabilitazione delle connessioni con stesso alias ambienti on premise
- Rilascio sistemi.

5 DURATA E SEDE DELLA FORNITURA

La durata del contratto decorrerà dalla data di stipula fino allo spirare di **54 (Cinquantaquattro)** mesi, decorrenti dalla data di stipula.

La SAP CDC è l'elemento centrale del nuovo modello di attivazione e fruizione delle componenti SAP; l'attivazione del servizio richiede circa 6 mesi di preparazione dalla firma del contratto.

Nel rispetto degli obiettivi dell'Amministrazione, l'attivazione della SAP CDC dovrà avvenire entro e non oltre il 30 giugno 2026, o diverso termine eventualmente concordato con Sogei.

Si riporta di seguito la durata richiesta per ciascun servizio ricompreso nell'oggetto di fornitura.

SAP CDC

Oggetto	Durata del servizio	Note
SAP CDC – PRIVATE TAILORED OPTION CUSTOMER DATA CENTER (SAP CDC)		
SAP Cloud ERP Private, tailored option	48 mesi	Accensione stimata entro sei mesi dalla stipula del contratto
SAP Safekeeper	Dal 01.01.2026 fino al 31.12.2027	
SOFTWARE LIFECYCLE INDUSTRIALIZZATO		
SAP Data Custodian KMS	Stessa scadenza SAP CDC	
SAP Signavio	Stessa scadenza SAP CDC	
Tricentis	Stessa scadenza SAP CDC	
Servizi SAP Premium Engagement/Quality Assurance		
Servizi SAP Premium Engagement/Quality Assurance	24 mesi	Dalla stipula del contratto
Setup per supporto operativo		
Setup SAP Business Technology Platform	Fino all'accensione SAP CDC	Accensione stimata entro sei mesi dalla stipula del contratto
Setup SAP Analytics Cloud Planning	Fino all'accensione SAP CDC	Accensione stimata entro sei mesi dalla stipula del contratto
Setup Servizio di manutenzione on premise	Fino all'accensione SAP CDC	Accensione stimata entro sei mesi dalla stipula del contratto

SAP BTP

Oggetto	Durata del servizio	Note
SAP BTP (Post setup per supporto operativo)		
SAP BTP	Stessa scadenza SAP CDC	

SAP Analytics Cloud Planning

Oggetto	Durata del servizio	Note
SAP SAC (Post setup per supporto operativo)		
SAP SAC	Fino al 31/12/2026 con possibile interruzione anticipata in caso di dismissione della componente tecnologica	

Manutenzione residua post setup

Oggetto	Durata del servizio	Note
Manutenzione residua post setup		
Servizio di manutenzione on premise Post setup (componenti non incluse in SAP CDC)	Fino al 31.12.2027	

Le attività correlate alla fornitura/installazione ed erogazione della fornitura, avranno luogo presso la sede di Sogei, via Mario Carucci, 99, Roma.

Eventuali interventi presso altre sedi, site nel comune di Roma, potranno essere comunque richiesti da Sogei al fornitore del servizio.

6 MODALITÀ DI ESECUZIONE DELLA FORNITURA

Tutte le attività dovranno essere svolte in collaborazione con i referenti della Committente, secondo modalità che saranno opportunamente concordate in fase di avvio.

La Committente si riserva di modificare le modalità di esecuzione descritte e di introdurre nuove modalità, anche in corso d'opera, dandone congruo preavviso all'Impresa. In aggiunta, tali modalità di esecuzione potranno essere congiuntamente riviste, su proposta dell'Impresa, e potranno essere concordate opportune semplificazioni o variazioni in funzione delle specificità dei singoli interventi.

6.1 Consegna, installazione e configurazione della soluzione

Relativamente alla consegna delle sottoscrizioni oggetto di setup operativo della SAP CDC, il fornitore entro **5 (cinque) giorni** dalla stipula del contratto dovrà inviare via e-mail alla casella di posta ConsegnaSW@sogei.it, una "*Nota di Consegna*", che riporti al suo interno:

- la ragione sociale del Fornitore;
- il numero di repertorio del Contratto;
- la descrizione dettagliata dei prodotti, con i relativi quantitativi e il tipo, modello e numero seriale della versione dei prodotti software;
- (*eventuale*) le chiavi di attivazione delle sottoscrizioni fornite e/o i certificati di proprietà/utilizzo;
- (*eventuale*) le istruzioni e le credenziali per accedere al sito del produttore e poter scaricare il SW.

Relativamente alle componenti infrastrutturali e software della SAP CDC il fornitore entro **15 (quindici) giorni** dalla stipula del contratto dovrà presentare un "*Piano operativo*" contenente data di consegna, installazione, configurazione. Ai fini della corretta definizione da parte del fornitore della fornitura/servizio, potrà prevedersi un sopralluogo per la verifica propedeutica di sedi/locali/impianti presso i datacenter Sogei (data center primario, secondario). Il Piano Operativo dovrà essere approvato dalla Committente entro **15 (quindici) giorni** dall'avvenuta consegna dello stesso. La Committente potrà richiedere eventuali modifiche sui termini proposti nel piano operativo che dovranno essere recepite dal Fornitore entro il termine di **5 (cinque) giorni**, pena l'applicazione delle penali. I termini previsti nel Piano operativo approvato dalla Committente devono intendersi inderogabili, pena l'applicazione delle penali.

Si precisa che, per le componenti infrastrutturali, si dovranno concordare il luogo di consegna della fornitura giorno della settimana e fasce orarie di disponibilità per la ricezione della fornitura stessa

Ultimate le eventuali operazioni di installazione, la Committente produrrà il “*Rapporto di Fine Installazione*”, o altro documento equipollente, recante le seguenti indicazioni: tipo, modello e numero seriale delle apparecchiature hardware installate, sistema operativo, *part number* e modalità di *licensing* dei prodotti software installati, nonché la dichiarazione di rispondenza dei prodotti forniti alle specifiche di cui al presente Capitolato Tecnico.

Nel caso in cui il Fornitore, per cause allo stesso imputabili, non rispetti i termini indicati nel “*Piano Operativo*”, Sogei applicherà le penali secondo le modalità indicate nello Schema di contratto.

Dovranno inoltre essere a totale carico dell’Impresa, intendendosi ricompresi nei corrispettivi corrisposti, tutti gli oneri relativi alle attività ed agli adempimenti occorrenti all’integrale espletamento dell’oggetto contrattuale, ivi compresi le eventuali spese di trasporto, di viaggio e di missione per il personale addetto al sopralluogo ed all’esecuzione dei servizi ed i connessi oneri assicurativi.

Relativamente alle licenze in sottoscrizione incluse nella SAP CDC il Fornitore si impegna ad informare la Committente delle eventuali variazioni dei prodotti che dovessero intervenire nel corso di validità contrattuale.

L’accettazione definitiva è subordinata all’esito positivo della verifica di conformità (cfr. par. 7) nonché ai test previsti dal CVCN (di cui al paragrafo 4.10.3), pena la risoluzione del contratto.

6.2 Erogazione del servizio di manutenzione

L’Impresa dovrà garantire l’erogazione del servizio di manutenzione, fino alla scadenza del contratto, e quindi fino ad un massimo di 54 (cinquantaquattro) mesi con le modalità ed i livelli di servizio indicati nel presente paragrafo, della fornitura di cui al paragrafo 3.

La soluzione dovrà essere oggetto di manutenzione correttiva consistente nella fornitura di quanto necessario (nuove versioni del software/firmware, *patch* o *workaround*) in grado di risolvere eventuali problemi funzionali o di sicurezza che si manifestino nell’uso del prodotto.

Dovranno essere forniti gli aggiornamenti del sistema (es. per *patch*, nuove *release*) oltre all’aggiornamento di quanto necessario ad intercettare eventuali vulnerabilità presenti tra gli artefatti e le immagini depositate nel *repository*.

Tutte le attività già menzionate da erogare a partire dalla “*Data di Accettazione della fornitura*”, fino al termine della stessa, dovranno essere comprese nella soluzione.

Le componenti oggetto della fornitura, di cui al par. 3 del presente documento, prevedono livelli di servizio differenti in base alla tipologia di prodotto SAP.

Con riferimento alle sottoscrizioni attivate, si richiede il rispetto dei livelli di servizi richiesti di seguito che sarà rilevato dallo strumento di monitoraggio *SAP for Me* che sarà messo a disposizione dal fornitore.

Si riportano di seguito il dettaglio dei livelli di servizio:

Livelli di servizio	Soglia	Periodicità	Modalità di erogazione
SAP CDC ambienti produttivi	99,9%	Mensile	Rilevazione sullo strumento di monitoraggio <i>SAP for Me</i>
SAP CDC Ambienti non-Prod	98%	Mensile	Rilevazione sullo strumento di monitoraggio <i>SAP for Me</i>
SAP <i>Business Technology Platform</i> – servizio <i>SAP Workzone Standard Edition</i>	99,95%	Mensile	Rilevazione sullo strumento di monitoraggio <i>SAP for Me</i>
SAP <i>Analytics Cloud</i>	99,7%	Mensile	Rilevazione sullo strumento di monitoraggio <i>SAP for Me</i>
SAP <i>Signavio</i>	99,7%	Mensile	Rilevazione sullo strumento di monitoraggio <i>SAP for Me</i>
SAP <i>Data Custodian</i>	99,7%	Mensile	Rilevazione sullo strumento di monitoraggio <i>SAP for Me</i>

Nel contesto Sogei, sono da ritenere sospesi gli SLA per la SAP CDC in caso di:

- attivazione della presa in carico dei sistemi da parte di Sogei (procedura “*Service Continuity Plan*”);
- ritardo da parte di Sogei del rilascio dell’utenza *SAPHANADB* in caso di *downtime* riconducibile a problematiche legate a questa utenza.

Calcolo disponibilità sistema/servizio

Di seguito si riporta il calcolo sulla disponibilità del sistema:

- *Percentuale di disponibilità di sistema = (Totale minuti mese – tempo di fermo escluso «finestra manutenzione» – Tempo di fermo «downtime») / (Totale minuti mese – tempo di fermo escluso «finestra manutenzione»)*
“Downtime” si riferisce al Totale di Minuti al Mese di indisponibilità dell’applicazione,
“Finestra di Manutenzione” si riferisce alle finestre di manutenzione da concordare con Sogei, dove SAP potrà eseguire attività di manutenzioni delle applicazioni (es. applicazioni patch di sicurezza).

Tempi di risposta agli incident

Di seguito si riportano i tempi di risposta previsti per gli *incident*:

Priorità	Tempo di reazione all’incidente (IRT)	SLA per IRT
1 – Molto Alta	Il tempo di reazione parte da quando il Livello 1 di Supporto SAP è contattato per l’incidente e la prima azione è intrapresa dalla persona del support SAP per la risoluzione dello stesso.	20 minuti (7*24h) (piano di risoluzione del problema entro 4 ore)
2 – Alta		2 ore
3 – Medio		4 ore
4 – Bassa		1 Giorno Lavorativo

Penali

Nel caso in cui non venga rispettato lo SLA relativo alla Disponibilità di Sistema nel corso di uno specifico Mese, Sogei avrà diritto di farsi riconoscere un credito, pari al 2% del Corrispettivo Mensile per ogni decimo di punto % sotto lo SLA da imputarsi sulla fattura successiva; tale credito non sarà superiore al 100% dei corrispettivi pagati nel mese di pertinenza.

Il credito sarà richiesto tramite il Technical Service Manager di SAP o il fornitore.

6.3 Erogazione dei servizi di supporto specialistico

I servizi specialistici compresi nella SAP CDC, ed erogati dal software vendor SAP, prevedono il supporto specialistico di figure professionali di casa madre, per tutte le esigenze specifiche legate all'implementazione, installazione, configurazione ed erogazione della soluzione oggetto della fornitura, come descritto nel paragrafo 4.4 del presente Capitolato.

I servizi professionali saranno svolti prevalentemente da remoto, salvo diversa indicazione di Sogei, che potrà chiederne lo svolgimento anche presso la propria sede, ovvero presso altre sedi.

L'erogazione dei servizi dovrà avvenire nelle modalità descritte nel precedente paragrafo 4.4.

Ogni attività ed intervento richiesto ed erogato prevederà la compilazione di un report "*Elenco degli interventi e Consuntivo attività*", che verrà consegnato alla Sogei nel corso dell'esecuzione delle prestazioni e sottoposto all'approvazione di Sogei stessa, che verificherà la quantificazione nonché la corretta esecuzione dei servizi. L'"*Elenco degli interventi e Consuntivo attività*" dovrà riportare, relativamente al servizio di supporto specialistico nel periodo di riferimento, almeno le seguenti informazioni:

- la descrizione dettagliata delle attività eseguite;
- valutazione qualitativa delle attività eseguite;
- le date ovvero i periodi in cui le attività sono state eseguite.

A fronte della consegna del "*Elenco degli interventi e Consuntivo attività*", Sogei procederà alla verifica di conformità dei servizi erogati.

6.3.1 Approvazione e sostituzione delle figure professionali

Entro **5 (cinque) giorni lavorativi** dalla richiesta da parte di Sogei, il Fornitore dovrà inviare a Sogei nominativi e curricula delle figure professionali SAP che saranno impiegate. Il Fornitore dovrà garantire la disponibilità delle risorse SAP individuate alla data di invio dei predetti curricula o ad altra data indicata dalla Committente.

La Committente, in qualunque momento della durata contrattuale, potrà chiedere a mezzo e-mail la sostituzione delle figure professionali SAP non ritenute idonee allo svolgimento delle

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

attività ed il Fornitore si impegna a procedere a richiederne la sostituzione con altre risorse aventi almeno i requisiti minimi di cui al paragrafo 4.4.

L'idoneità oppure la non idoneità delle risorse SAP impiegate sarà verificata da Sogei in riferimento al buon esito degli output ricevuti sulle attività eseguite e relazionate nel "*Elenco degli interventi e Consuntivo attività*" nell'ambito dei servizi di supporto specialistico di cui al presente Capitolato Tecnico.

Entro **5 (cinque) giorni lavorativi** dalla richiesta di sostituzione inoltrata da Sogei, o nel diverso termine eventualmente indicato dalla Committente, il Fornitore dovrà inviare ad Sogei i curricula delle nuove risorse SAP da impiegare le quali dovranno possedere i requisiti minimi di cui al paragrafo 4.4.

Anche in questo caso, il Fornitore dovrà garantire la disponibilità delle nuove risorse SAP individuate alla data di invio dei predetti curricula o ad altra data indicata dalla Committente.

L'eventuale sostituzione dei professionisti non comporterà alcun onere aggiuntivo per la Committente.

In caso di mancata sostituzione delle risorse SAP ritenute non idonee, o in caso di sostituzione oltre il termine di **10 (dieci) giorni lavorativi**, o in caso di inidoneità della risorsa SAP sostituita, la Committente applicherà la relativa penale:-

6.4 Responsabile della Fornitura e Modalità di comunicazione

L'Impresa aggiudicataria dovrà comunicare ai fini della stipula il nominativo e i riferimenti del proprio Responsabile della Fornitura, il quale assume il ruolo di referente per tutte le attività previste dal presente Capitolato Tecnico, con la responsabilità di gestire e risolvere tutte le problematiche tecniche e contrattuali legate al corretto svolgimento della fornitura affinché la Sogei, nella persona del proprio Direttore dell'esecuzione, possa farvi riferimento per ogni aspetto riguardante le attività di seguito descritte.

L'Impresa si impegna a comunicare, contestualmente alla stipula del contratto, un indirizzo e-mail, un numero di telefono e/o un sito Web al quale rivolgersi, per ogni comunicazione relativa alla fornitura.

Il Responsabile della Fornitura dell'Impresa sarà l'interlocutore unico della Sogei per gli aspetti amministrativi, per l'organizzazione ed il coordinamento delle attività contrattuali. Sarà cura del responsabile verificare il rispetto di tutti gli adempimenti contrattuali.

Per facilitare e velocizzare l'attività amministrativa di entrambe le parti, ogni comunicazione riguardante aspetti contrattuali dovrà essere scambiata, sia in formato cartaceo che elettronico, tra il responsabile Sogei e quello dell'Impresa.

Per tutta la durata contrattuale, l'Impresa dovrà garantire la piena funzionalità dei mezzi di comunicazione sopraindicati comunicando tempestivamente a Sogei eventuali modifiche.

7 VERIFICA DI CONFORMITÀ

La **verifica di conformità** ha l'obiettivo di accertare l'avvenuta attivazione del servizio e che quest'ultimo sia conforme con quanto previsto in termini contrattuali; nel dettaglio saranno verificati gli aspetti relativi a SW, *sizing* dei sistemi e gli altri aspetti legati all'erogazione del servizio SAP CDC.

La verifica di conformità verrà eseguita:

- a) con riferimento supporto operativo in fase di setup, di cui al paragrafo 4.1, **entro 5 (cinque) giorni lavorativi**, successivi alla ricezione della "*Nota di Consegna*" (cfr. par. 6.1) inviata dal fornitore. Il controllo verterà consistere nel controllo, tramite apposito strumento di monitoraggio, della disponibilità di tutte le funzionalità/prodotti richiesti e sulla presa in carico del supporto operativo. La positiva conclusione della verifica comporterà l'accettazione dei prodotti da parte di Sogei e determinerà la specifica "*Data di accettazione della Fornitura*";
- b) con riferimento alla verifica di avvio della soluzione SAP CDC (una tantum post installazione/configurazione di base dei primi sistemi propedeutica all'avvio del progetto di *move*) della soluzione **entro 6 mesi dalla data di stipula contrattuale, comunque entro e non oltre 10 giorni lavorativi** successivi al "*Rapporto di Fine Installazione*" (cfr. par. 6.1), ed ha l'obiettivo di verificare l'effettiva attivazione del servizio, ponendo l'attenzione anche sulle specifiche tecniche e componenti software. I test saranno eseguiti su ambienti *skeleton* che saranno previsti al momento dell'avvio del servizio, ovvero ambienti installati ex-novo che costituiranno la base di partenza per effettuare successivamente la migrazione, e seguiranno il piano di rilascio dei vari ambienti.

Le principali verifiche che saranno eseguite e documentate in fase di avvio sono:

- Raggiungibilità dei server da rete Sogei
- Specifiche tecniche di *sizing* (CPU e RAM)
- Specifiche tecniche di sistema operativo (versione)
- Specifiche tecniche del *database* (dimensioni e versione)
- Specifiche tecniche del SID (System ID) dell'applicazione SAP (ove previsto)

Inoltre, sarà possibile verificare la disponibilità delle licenze SW della SAP CDC sul portale SAP for me (<https://me.sap.com/>).

Il dettaglio delle verifiche, le modalità e dei sistemi/servizi oggetto di verifica (totale o a campione) sarà definito dalle parti in base al piano di rilascio.

La verifica verterà anche sull'erogazione dei servizi specialistici e del relativo "*Elenco degli interventi e Consuntivo attività*".

La positiva conclusione della verifica comporterà l'accettazione dei prodotti da parte di Sogei e determinerà la specifica "*Data di accettazione della Fornitura*";

- c) con riferimento alla verifica ricorrente di disponibilità della soluzione SAP CDC in versione target (da ripetersi ad **ogni trimestre dall'avvio**) Costituisce la verifica di

conformità sul servizio a regime ed ha l'obiettivo di constatare l'effettiva rispondenza del servizio contrattualizzato con la disponibilità dello stesso.

In questa verifica, trovandosi in una situazione a regime, sarà possibile effettuare su tutti i sistemi in ambito:

- le principali verifiche descritte per la fase di avvio
- la verifica sul livello di servizio erogato per le soluzioni SAP in ambito
- la verifica delle quantità sottoscritte di licenze SW SAP
- i test di funzionalità della soluzione, in particolare:
 - Verifica raggiungibilità dei sistemi attraverso un accesso all'applicazione SAP tramite *SAPGui* oppure tramite pagina HTTP
 - Verifica licenza SAP installata su Database e Applicazione SAP
 - Verifica livello applicativo SAP
 - Verifica esecuzione *policy* di *backup*
- le verifiche sul funzionamento di meccanismi di *fault tolerance* (HA/DR) dove previsto, in particolare:
 - Esecuzione test di funzionamento della *fault tolerance* sui servizi Database e SAP *Central Services* conformemente allo standard definito in SAP CDC
 - Esecuzione test per verificare il corretto funzionamento dei meccanismi di replica dei database/application server ed esecuzione di un test di *Disaster Recovery (failover)*

La verifica verterà anche sull'erogazione dei servizi specialistici e del relativo "*Elenco degli interventi e Consuntivo attività*".

Il dettaglio delle verifiche, le modalità e dei sistemi/servizi oggetto di verifica (totale o a campione) sarà definito e concordato dalle parti.

- d) con riferimento alla fornitura delle Sottoscrizioni SAP SAC – SAP Analytics Cloud, di cui al paragrafo 4.7, la verifica di conformità dovrà avvenire entro il termine di **10 giorni lavorativi** successivi al "*Rapporto di Fine Installazione*" (cfr. par. 6.1) e consisterà nel controllo della disponibilità da parte della Committente delle relative quantità per le soluzioni oggetto della fornitura all'interno del portale SAP for me (<https://me.sap.com/>). La positiva conclusione della verifica comporterà l'accettazione dei prodotti da parte di Sogei e determinerà la specifica "*Data di accettazione della Fornitura*".
- e) con riferimento alla fornitura delle Sottoscrizioni SAP BTP – SAP Business Technology Platform e SAP Analytics Cloud, di cui al paragrafo 4.8, la verifica di conformità dovrà avvenire entro il termine di **10 giorni lavorativi** successivi al "*Rapporto di Fine Installazione*" (cfr. par. 6.1), e sarà ripetuta ogni trimestre, e consisterà nel controllo della disponibilità da parte della Committente delle relative quantità per le soluzioni oggetto della fornitura all'interno del portale SAP for me (<https://me.sap.com/>). La positiva conclusione della verifica comporterà l'accettazione dei prodotti da parte di Sogei e determinerà la specifica "*Data di accettazione della Fornitura*".

- f) con riferimento alla fornitura manutenzione on premise residua, di cui al paragrafo 4.9, la verifica di conformità verrà effettuata a partire dal termine di **10 giorni lavorativi** successivi al “*Rapporto di Fine Installazione*” (cfr. par. 6.1), e sarà ripetuta ogni trimestre, e consisterà nel controllo della disponibilità all’interno dell’apposito strumento di monitoraggio di tutte le funzionalità richieste. La positiva conclusione della verifica comporterà l'accettazione dei prodotti da parte di Sogei e determinerà la “*Data di accettazione della Fornitura*”.

Delle operazioni di verifica di conformità verrà redatto apposito verbale. La verifica di conformità si intenderà positivamente superata solo nel caso in cui le prestazioni risultino eseguite a regola d’arte, sotto il profilo tecnico-funzionale, e in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato Tecnico e nel contratto, nonché secondo le indicazioni di Sogei.

Il Fornitore è tenuto a prestare a Sogei, a propria cura e spese, l’assistenza tecnica necessaria e a mettere a disposizione della Committente le attrezzature eventualmente occorrenti alle operazioni di verifica di conformità.

Il Fornitore potrà intervenire durante la verifica di conformità, anche attraverso propri rappresentanti. In tal caso detti rappresentanti saranno tenuti a sottoscrivere i documenti di verifica di conformità che verranno redatti da Sogei (verbali, certificato, ecc.).

In caso di esito negativo della verifica di conformità, l’Impresa dovrà provvedere, a propria cura e spese, ad eliminare i vizi accertati entro il termine massimo che le verrà comunicato dalla Sogei in sede di verbale verifica di conformità, fatto salvo quanto previsto nei prescritti livelli di servizio. In tale ipotesi, la verifica di conformità verrà ripetuta con le modalità precedentemente descritte.

Nel caso in cui anche la seconda verifica di conformità desse esito negativo, la Sogei, ferma l’applicazione delle penali, avrà facoltà di risolvere il contratto.

Tutti gli oneri derivanti dalla verifica di conformità si intendono a carico dell’Impresa.

7.1 Test CVCN

La **verifica di conformità** ai test previsti dal CVCN (di cui al paragrafo 4.10.3) ha l’obiettivo di accertare il positivo superamento dei test individuati dal CVCN. In particolare:

- a) i test previsti dal CVCM, di cui al paragrafo 4.10.3, dovranno concludersi **entro 6 mesi dalla stipula**, prelieve le verifiche preliminari sulla soluzione SAP CDC ai sensi dell’art. 4, comma 3 e dell’art 5, comma 3, del DPR 5 febbraio 2021, n. 54, **e comunque prima dell’attivazione della soluzione SAP CDC**, e verteranno su:
- verifica della corretta implementazione delle funzionalità di sicurezza;
 - verifica di intrusione, a supporto dell’analisi di vulnerabilità.

I test dovranno concludersi non oltre 60 giorni decorrenti dal momento in cui l'ambiente di test risulterà predisposto.

Il CVCN comunicherà l'esito delle operazioni di verifica di conformità ai test CVCN.

La verifica di conformità si intenderà positivamente superata solo nel caso in cui le prestazioni risultino eseguite a regola d'arte, sotto il profilo tecnico-funzionale, e in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato Tecnico e nel contratto, nonché secondo le indicazioni di Sogei e del CVCN.

Il Fornitore è tenuto a prestare a Sogei ed al CVCN, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione della Committente le attrezzature eventualmente occorrenti alle operazioni di verifica di conformità ai test previsti dal CVCN.

Il Fornitore potrà intervenire durante la verifica di conformità ai test previsti dal CVCN, anche attraverso propri rappresentanti. In tal caso detti rappresentanti saranno tenuti a sottoscrivere i documenti di verifica di conformità ai test previsti dal CVCN che verranno redatti da Sogei (verbali, certificato, ecc.) e dal CVCN.

In caso di esito negativo della verifica di conformità ai test previsti dal CVCN, l'Impresa dovrà provvedere, a propria cura e spese, ad eliminare i vizi accertati entro il termine massimo che le verrà comunicato dalla Sogei e dal CVCN. In tale ipotesi, la verifica di conformità ai test previsti dal CVCN verrà ripetuta con le modalità precedentemente descritte e secondo quanto previsto dal DL 105/2019 e dal DPR 5 febbraio 2021, n. 54.

Nel caso in cui anche le successive verifiche di conformità ai test previsti dal CVCN dessero esito negativo e il CVCN dichiarasse l'impossibilità a procedere ulteriormente con i test, si applicheranno le disposizioni in tema di risoluzione del contratto.

Tutti gli oneri derivanti dalla verifica di conformità ai test previsti dal CVCN si intendono a carico dell'Impresa.

8 PORTALE FORNITORI

Sogei nel rapporto con i fornitori promuove sempre nuove sinergie allo scopo di ottimizzare i risultati attraverso una gestione dei contratti tracciata e strutturata. A tal fine mette a disposizione il Portale dei fornitori, strumento informatico che permette di gestire e razionalizzare i processi. Il portale fornitori è raggiungibile tramite internet e stabilisce un punto di colloquio per lo scambio della documentazione in fase di esecuzione contrattuale, con particolare riferimento ai contratti di esternalizzazione di sviluppo software. Facilita l'interazione e la collaborazione fra le parti, velocizzando i tempi di gestione amministrativa degli adempimenti, permette di monitorare lo stato di avanzamento delle attività, di dematerializzare la documentazione e ottimizzare le attività di consuntivazione.

Il portale gestisce, in particolare, le seguenti fasi contrattuali:

- Accreditamento del personale – Attività necessaria affinché il personale coinvolto possa accedere ai sistemi Sogei o presso le sedi Sogei.
- Ciclo di vita degli affidamenti di sviluppo software (verbale di affidamento, verbale di consegna, verbale di verifica di conformità);
- Rilevazione attività e produzione dei dati utili alla Fatturazione elettronica (dati FEP);
- Gestione Subappalto in fase di esecuzione (trasmissione fatture quietanzate).

La Sogei si riserva di implementare altri metodi di rendicontazione delle prestazioni al fine di rendere più efficiente il servizio.

Per ulteriori informazioni relativamente alle modalità di abilitazione e di accesso al portale si rimanda [alla pagina dedicata presente sul sito Sogei nell'area fornitori](#).

8.1 Accreditamento del personale

Tutte le risorse coinvolte nell'esecuzione contrattuale, siano esse dipendenti o collaboratori o liberi professionisti della società aggiudicatrice o, ancora, dipendenti o collaboratori o liberi professionisti dell'eventuale ausiliaria o dell'eventuale subappaltatore, ai fini della loro abilitazione all'accesso sui sistemi Sogei o per l'ingresso nelle sedi Sogei dovranno essere accreditate attraverso la sezione "Accreditamenti" presente sul **Portale fornitori**, strumento informatico messo a disposizione da Sogei.

ALLEGATO 1 – LINEE GUIDA SERVICE CONTINUITY PLAN

Introduzione

Il presente piano ha l'obiettivo di definire le procedure e le modalità di attivazione del *Service Continuity Plan* per il servizio SAP CDC, erogato in modalità remota attraverso un modello a servizio che non consente l'accesso a Sogei ad alcune componenti della soluzione su cui il servizio si poggia. Il *Service Continuity Plan* viene attivato in situazioni eccezionali in cui SAP è impossibilitata ad accedere allo stesso sia in modalità remota che attraverso personale *on-site* o in casi di forza maggiore che richiedono il passaggio del completo controllo a Sogei/l'Amministrazione per garantire la continuità operativa. Questo scenario è da considerarsi eccezionale, cosa che comporta la deroga di tutti i livelli di servizio contrattualizzati, tra Sogei/l'Amministrazione e il fornitore, per tutto il periodo in cui il piano di *Service Continuity* rimarrà attivo.

Tale procedura è da considerarsi eccezionale e necessaria a rispondere alle normative di legge Italiane inerenti alla gestione dei dati che rientrano nel "Perimetro Nazionale di Sicurezza Cibernetica" (PNSC).

Modello funzionale del *Service Continuity Plan*

La soluzione SAP CDC è un servizio il cui scopo è fornire un ambiente applicativo SAP autoconsistente.

SAP in questo contesto configura e gestisce le componenti, infrastruttura inclusa, necessarie all'erogazione del servizio ad esclusione della componente legata al luogo fisico in cui la soluzione viene implementata (*Data Center*).

In questo contesto, Sogei/l'Amministrazione ha la responsabilità di:

- *Facility* in cui viene ospitata la soluzione;
- *Power e Cooling*;
- *Network* di integrazione della soluzione rispetto alla rete di Sogei/dell'Amministrazione;
- Sicurezza fisica e perimetrale.

Il servizio è normato da "*Service Level Agreement*" contrattualizzati dal fornitore e soggetti a specifiche penali.

Per garantire gli SLA contrattuali sono definiti i confini di accesso alla soluzione da parte di Sogei/l'Amministrazione NON consentendo a quest'ultimo l'accesso a:

- Sistema operativo dei vari *host*;
- Componente di virtualizzazione (*Hypervisor*);
- Componenti di *networking* fisiche e virtuali;

- Sistemi *Storage*;
- Sistema di *backup*;
- *Backup repository*.

Il *Service Continuity Plan* in questo contesto delinea una condizione eccezionale in cui, sulla base dei “Casi di attivazione” previsti nel presente allegato, si attiverà una procedura specifica che renderà disponibile ad un elenco di persone di Sogei/l’Amministrazione l’accesso completo alla soluzione in tutte le componenti sopra indicate che in condizioni normali non sono accessibili dal Sogei/dall’Amministrazione.

SAP fornisce tutte le credenziali e la documentazione necessari per garantire l’accesso completo alla soluzione garantendo, ove possibile, un supporto per eventuali necessità legate ad informazioni o chiarimenti necessari a Sogei/all’Amministrazione per un accesso fattivo alla soluzione.

Una volta attivata la procedura, SAP non sarà più responsabile dell’esercizio della soluzione, che sarà demandata in toto a Sogei/l’Amministrazione, incluse le attività legate alla resilienza del servizio quali:

- Servizio di *backup*;
- Servizio di *monitoring*;
- Servizio di *Disaster Recovery*.

In tale circostanza i vincoli contrattuali legati agli SLA verranno sospesi e il partner fornitore verrà esentato dal pagamento di qualsivoglia penale contrattuale legata al mancato rispetto degli stessi.

Casi di Attivazione del *Service Continuity Plan*

Le casistiche di attivazione del servizio sono legate al rispetto di quanto espresso all’interno del riferimento normativo decreto-legge 21 settembre 2019, n. 105 che definisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) e sancisce le responsabilità di Sogei di tutelare i propri beni ICT il cui malfunzionamento causerebbe l’interruzione totale o una compromissione dei servizi offerti alla Pubblica Amministrazione.

In tale contesto l’attivazione del *Service Continuity Plan* è un atto formale che prevede la comunicazione, quando possibile, da parte di Sogei verso il fornitore ed il software vendor SAP della necessità di attivare tale piano e della motivazione per cui Sogei intende attivarlo.

L’attivazione tecnica del *Service Continuity Plan* sarà realizzabile in totale autonomia da parte di Sogei senza un intervento diretto di SAP, per questo motivo saranno poste in essere adeguate procedure tecniche che consentiranno a Sogei, anche in assenza di comunicazione remota e locale con SAP, di mettere in essere tale Piano e quindi consentire l’accesso amministrativo alle componenti tecnologiche sottostanti al servizio.

L'accesso amministrativo sarà normalmente non attivo, Sogei avrà disponibilità di opportune procedure che oltre ad attivare tecnicamente l'accesso necessario tratteranno in modo univoco il momento dell'attivazione del *Service Continuity Plan*.

A titolo esemplificativo e non esaustivo, si elencano alcune possibili motivazioni che portano all'attivazione del *Service Continuity Plan*:

- a) Impossibilità di SAP di accedere remotamente al servizio e di fornire un supporto alternativo locale.
- b) Situazioni di forza maggiore che costringono la Sogei/l'Amministrazione ad esonerare SAP dall'accesso al servizio:
 - a. Necessità di isolare completamente l'esercizio da parte di Sogei/dell'Amministrazione per questioni di sicurezza interna;
 - b. Necessità di isolare completamente l'esercizio da parte di Sogei/dell'Amministrazione per questioni di sicurezza nazionale;
 - c. Identificazione dell'erogatore del servizio come soggetto non gradito per questioni di sicurezza;
 - d. Identificazione dell'erogatore del servizio come soggetto non gradito per questioni reputazionali;
 - e. Situazione di crisi fra Italia e Germania che interrompono le relazioni istituzionali fra le parti.

Procedure di Attivazione del *Service Continuity Plan*.

Soddisfatti i requisiti di cui alla successiva appendice A, sarà possibile attivare la procedura di *Service Continuity Plan* nei termini che seguono:

- a) In modalità preventiva verranno concordate con Sogei le utenze in grado di accedere in modalità amministrativa ai sistemi. Tali utenze saranno in numero di due e dovranno essere associate a persone fisiche Sogei che ne avranno la responsabilità. Tali utenze saranno sempre attive sui sistemi e sarà cura di Sogei garantirne il corretto funzionamento tramite cambio periodico delle password ogni 3 mesi.
- b) Sogei/l'Amministrazione dichiara formalmente la situazione di criticità invocando il *Service Continuity Plan*.
- c) Sogei/l'Amministrazione notifica, quando possibile, al partner fornitore e all'erogatore del servizio l'attivazione del *Service Continuity Plan* indicandone la motivazione.
- d) Attraverso l'accesso locale ad un terminale predisposto a questi scopi (*zero trust WTS*) e messo a disposizione da Sogei, verranno attivate le regole di sicurezza *firewall* e di *routing*, che consentiranno l'accesso amministrativo solo e soltanto attraverso tale terminale, da quel momento in poi si attiveranno le condizioni descritte nel paragrafo "Accettazione e Condizioni del *Service Continuity Plan*".

Classificazione del documento: Consip Public

Appalto specifico indetto da Consip S.p.a. per l'acquisizione della soluzione SAP CDC per Sogei ID – 2925

Allegato 2 - Capitolato tecnico

- e) Verrà attivata da Sogei la registrazione di tutte le attività svolte attraverso tale terminale in modo da tenere traccia di qualsiasi modifica verrà fatta sui sistemi fino al rientro nelle modalità operative standard previste dal servizio.
- f) Se possibile, una figura preposta da SAP sarà incaricata di supportare Sogei e sarà fisicamente presente negli uffici da Sogei/dall'Amministrazione durante il trasferimento di responsabilità.

La procedura è in fase di definizione, la proposta sopra descritta è indicativa e verrà affinata nel corso dei mesi antecedenti all'attivazione della SAP CDC.

Accettazione e Condizioni del *Service Continuity Plan*

L'attivazione del *Service Continuity Plan* richiede l'accettazione reciproca tra il fornitore e Sogei/l'Amministrazione, per tutta la durata della condizione di *Service Continuity Plan*, delle seguenti condizioni:

1. Il fornitore è esentato dal rispetto delle SLA contrattuali.
2. Il fornitore è esentato dal rispetto dei termini indicati dal *Data Protection Agreement*
3. L'erogatore del servizio è esentato dall'esercizio del servizio nonché dal rispetto delle specifiche di servizio legate al mantenimento del *Disaster Recovery*.
4. Il software vendor SAP è esentato dal rispetto delle specifiche di servizio legate al Backup Management.
5. Il software vendor SAP è esentato dalla gestione di qualsiasi attività di manutenzione hardware.
6. Sogei/l'Amministrazione si impegna a tenere traccia di tutti i cambiamenti e le modifiche che effettuerà sui sistemi durante il periodo di gestione autonoma.
7. Sogei/l'Amministrazione mantiene l'obbligo di pagamento dei costi del servizio come previsto nel contratto.
8. Il rientro alla normale operatività sarà a discrezione dell'erogatore del servizio e conforme a quanto descritto nel paragrafo "Rientro al Normale Esercizio del Servizio".

Rientro al Normale Esercizio del Servizio

Al termine dello stato di emergenza, riprenderà l'erogazione normale del servizio, con ripresa di tutti gli obblighi contrattuali e operativi del servizio SAP CDC.

Tale riattivazione è soggetta alla accettazione esplicita da parte di SAP che:

- a) Condurrà un assesment per valutare lo stato della soluzione, considerando eventuali modifiche apportate da Sogei/dall'Amministrazione durante il periodo di controllo autonomo.

- b) Sulla base dei risultati dell'assessment identificherà gli eventuali scostamenti dal modello operativo standard.
- c) Definirà un piano di intervento per riportare le soluzioni nelle condizioni necessarie alla presa in carico del servizio.
- d) Definirà le tempistiche necessarie all'implementazione del piano di intervento.
- e) Condividerà con Sogei/l'Amministrazione il piano e le tempistiche per l'accettazione.
- f) Eseguirà tutte le attività in collaborazione con Sogei/l'Amministrazione.
- g) Sospenderà qualsiasi possibilità di accesso a Sogei/all'Amministrazione alle componenti non consentite.
- h) Dichiarerà il rientro all'operatività.

Saranno a carico di Sogei/dell'Amministrazione i costi legati:

1. All'assessment definito al punto b.
2. Al progetto necessario per implementare le modifiche per il rientro alla normalità.

Appendice A. Pre-Requisiti tecnici

SAP dovrà:

- Creare gli utenti *c-users* (*Firefigther* user) e condividere le credenziali con Sogei/l'Amministrazione
- Definire un nuovo gruppo di accesso sulla piattaforma di controllo degli accessi (CAM) con delle regole di accesso predefinite sull'infrastruttura SAP CDC fornita a Sogei/all'Amministrazione.
- Fornire a Sogei/all'Amministrazione l'accesso ad un WTS all'interno della rete di gestione SAP attraverso gli utenti *c-users* definiti all'interno del dominio *hecadm*.
- Verificare che tali utenti possano accedere solo e soltanto alle componenti infrastrutturali previste per il Sogei/l'Amministrazione.
- Definire con il Sogei/l'Amministrazione una sottorete IP /27 o /28 (*Customer Control Network*) all'interno del piano di indirizzamento cliente che sarà autorizzata a veicolare traffico di rete di tipo amministrativo verso i sistemi SAP CDC.

Sogei/l'Amministrazione dovrà:

- Identificare due persone fisiche a cui verranno associate le due utenze *c-user* e che dovranno accettare le politiche di sicurezza SAP relative alla gestione delle utenze.
- Fornire una share condivisa accessibile solo dai due persone fisiche identificate dove verrà condiviso il materiale tecnico necessario alla gestione della procedura tecnica di subentro.

- Implementare due terminali WTS, *Zero Trust*, connessi alla rete di Sogei/dell'Amministrazione ed integrati nella sottorete /27 /28 CCN.