

CAPITOLATO TECNICO

SOLUZIONE DISASTER RECOVERY PER ACTIVE DIRECTORY

INDICE

1	DEFINIZIONI	3
2	PREMESSA.....	3
3	OGGETTO E DURATA.....	3
4	CARATTERISTICHE DELLA FORNITURA.....	4
5	MODALITÀ DI ESECUZIONE DEL CONTRATTO.....	5
5.1	LICENZE SOFTWARE DISASTER RECOVERY PER A.D.	5
5.2	SERVIZIO DI INSTALLAZIONE, CONFIGURAZIONE E MESSA IN ESERCIZIO.....	5
5.3	DELIVERABLE	6
5.4	SERVIZIO DI MANUTENZIONE	6
5.5	SERVIZI PROFESSIONALI	6
6	LUOGO DI SVOLGIMENTO DEL SERVIZIO.....	6
7	RESPONSABILE DELLA FORNITURA	6
8	MODALITÀ DI COMUNICAZIONE.....	7
9	ADEMPIMENTI PER LA SICUREZZA	7
10	OBBLIGHI DI RISERVATEZZA.....	7
11	VERIFICA DI CONFORMITÀ.....	7
12	MODALITÀ DI FATTURAZIONE E PAGAMENTO.....	7
13	LIVELLI DI SERVIZIO	8
14	PENALI	8

1 DEFINIZIONI

Nel corpo del documento, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- **Committente:** la Consip S.p.A.;
- **Capitolato tecnico:** il presente documento che enuncia le specifiche tecniche alle quali si dovrà conformare il Servizio;
- **Servizio:** il complesso delle attività oggetto del presente Capitolato;
- **Società/fornitore:** la Società o Impresa aggiudicataria del servizio;
- **Disaster Recovery:** le strutture tecnologiche e le procedure organizzative messe in atto per prevenire e contrastare/gestire “disastri”
- **Sistema eProcurement:** Sistema Informativo del Programma di Razionalizzazione degli Acquisti della P.A.;
- **Malfunzionamento:** qualsiasi errore, virus o codice malevolo o comunque difformità di funzionamento di Prodotti rispetto alla documentazione ed alle specifiche indicate nel presente Capitolato Tecnico;
- **Validazione temporale:** risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

2 PREMESSA

Consip, in qualità di società inclusa nell'elenco consolidato ISTAT, è soggetta agli impegni e adempimenti previsti dalla Legge 90/2024, relativamente alla gestione del rischio informatico, nonché dal capitolo 7 dal Piano Triennale per la PA 2024-2026 dell'AGID, relativo agli obiettivi di sicurezza informatica.

In ottemperanza alla Legge 90/2024, è stata condotta l'analisi del rischio informatico, nonché tenuto conto che, in ottemperanza all'obiettivo 7.3 Gestione e mitigazione del rischio cyber - RA7.3.1, del Piano Triennale AGID, è necessario prevedere la predisposizione di “piani e strumenti per garantirne la continuità operativa dei servizi offerti”, risulta essenziale per Consip dotarsi di uno strumento di Disaster Recovery per Active Directory (AD) affinché, a fronte di situazioni di emergenza che ne compromettano, anche in maniera parziale, la corretta erogazione, sia in grado di garantirne il ripristino completo, minimizzando i tempi di fermo dalla segnalazione dell'anomalia.

Nella fattispecie, Consip ha adottato una configurazione ibrida e articolata dell'AD, contenente più foreste e domini, che prevede parte dei componenti on premise, tra cui gli AD Domain Controller, installati sia nell'infrastruttura di sede che nella parte gestita da Sogei, parte dei componenti disponibile in Cloud attraverso il *tenant* assegnato da Microsoft a Consip.

3 OGGETTO E DURATA

L'implementazione di Disaster Recovery (DR) per l'Active Directory (AD), per il ripristino parziale e/o integrale di una o più foreste di Active Directory, oltre all'essere specificatamente progettato per il servizio MS Active Directory, deve prevedere requisiti essenziali quali:

- la possibilità di gestire il ripristino di configurazioni di AD complesse, anche installate su più siti o di tipo Cloud, in maniera automatizzata;
- la capacità di ridurre al minimo i tempi di ripristino;
- la possibilità di eseguire il ripristino in maniera flessibile, aggiornando o riparando unicamente la o le componenti del servizio AD che sono state compromesse.

La soluzione di DR per l'AD deve essere in grado di:

- utilizzare modalità di ripristino differenziate in funzione della gravità e dell'estensione del danno all'AD, ad es. ripristino integrale della foresta, ripristino Domain Controller AD, ripristino utenze AD danneggiate, ripristino Group Policy, ripristino attributi oggetto AD;
- consentire il ripristino della configurazione dell'AD Consip con più domini anche relazionati tra di loro, senza necessità di interventi o riconfigurazioni manuali;
- visualizzare ed evidenziare le differenze tra versioni differenti di backup dell'AD;
- adattare dinamicamente la configurazione dei Domain Controller in funzione dei server target disponibili.

La durata del contratto è pari a 36 mesi dalla "Data di accettazione dei servizi" (cfr. il successivo paragrafo n. 5.3 del presente Capitolato).

4 CARATTERISTICHE DELLA FORNITURA

Le caratteristiche principali del Disaster Recovery per l'Active Directory devono includere:

- Automazione: automatizzare il complesso processo di ripristino, eliminando l'elemento dell'errore umano. Disaster Recovery esegue le operazioni in parallelo e sincronizza le attività quando necessario, semplificando e accelerando il processo di ripristino.
- Flessibilità: Disaster Recovery offre un'ampia varietà di opzioni, da un metodo di ripristino partendo del sistema operativo pulito, al bare metal o al ripristino mediante golden image.
Le organizzazioni possono semplicemente rimuovere un controller di dominio dalla directory, promuoverlo in un sostituto, forzarne la retrocessione e/o promuoverlo nuovamente in qualsiasi momento. Gli amministratori possono configurare "pause" in ogni fase del ripristino per verificare o apportare modifiche alla configurazione prima di continuare il processo. RMADDRE garantisce che tutti i ruoli e le funzioni critiche siano integre e disponibili prima di confermare un ripristino riuscito.
- Maggiore sicurezza: Il ripristino su sistemi operativi puliti riduce la probabilità in cui potrebbero nascondersi malware non rilevati, riducendo la possibilità di infettare nuovamente Active Directory dai backup. La scansione automatizzata del malware consente di eseguire la scansione dei backup subito prima del ripristino.
- Maggiore efficienza e affidabilità dei backup di Active Directory: analizzare i backup nativi dello stato del sistema di Microsoft e ha rimosso tutti gli elementi non necessari per il ripristino di Active Directory. Ciò riduce la dimensione del backup, aumentando l'efficienza e l'affidabilità, oltre che impedire il backup del malware nascosto nella memoria del sistema utilizzando altre modalità di backup di Active Directory.
- Recupero graduale per ridurre l'obiettivo del tempo di ripristino (RTO): consentire alle organizzazioni di ripristinare le proprie Active Directory in più fasi. Il ripristino rapido dei controller di dominio (DC) più critici consente innanzitutto alle organizzazioni di avviare il ripristino dei servizi dipendenti da Active Directory e consentire rapidamente ai dipendenti l'accesso alle applicazioni chiave. Le organizzazioni possono aumentare la capacità, la disponibilità e l'affidabilità di Active Directory recuperando o aggiungendo controller di dominio nelle fasi successive.
- Backup crittografati: crittografare i backup per impedire ad autori malintenzionati di accedere a informazioni sensibili come le password o di alterare i backup.
- Backup protetti: un server hardenizzato completamente isolato, utilizzando regole IPSec, ed eseguire controlli per confermare l'integrità del backup. Anche se un'organizzazione subisce un attacco ransomware o perde i controller di dominio, l'archiviazione di livello 1 o il server Recovery Manager, l'organizzazione deve essere comunque in grado di eseguire il ripristino utilizzando i backup protetti nell'archiviazione protetta di Quest Secure Storage o dal cloud.

- Comparazione dei report di backup: offrire la possibilità di effettuare comparazioni confrontando lo stato di Active Directory live con i suoi backup, o confrontando più backup tra loro. Questo consente di accelerare il ripristino individuando rapidamente gli oggetti o gli attributi eliminati e/o modificati e di effettuare il ripristino senza impatti operativi.

5 MODALITÀ DI ESECUZIONE DEL CONTRATTO

5.1 LICENZE SOFTWARE DISASTER RECOVERY PER A.D.

Preso atto di quanto sopra descritta sarà predisposta ed implementata un'architettura di Disaster Recovery basata in grado di ripristinare l'operatività di Active Directory a seguito dei seguenti use case:

- Errore operativo day-by-day non critico
- Grave errore operativo / compromissione di attributi critici (password, SID History)
- Malware o compromissione dell'integrità della Directory

Lo scenario di disastro fisico di un server o di un Data Center, senza compromissione della Directory, è ripristinabile by design di MSFT. Non si ritiene pertanto di includerlo negli scenari di progetto.

Per indirizzare tali use case, la proposta preliminare di architettura prevede, l'implementazione di un singolo ambiente Quest RMAD DRE integrato con tutte le foreste ed i domini in perimetro, con lo scopo di garantire una gestione centralizzata e contenere l'impatto architetturale.

Il singolo ambiente potrà essere utilizzato dal Cliente per la gestione di tutti gli Use Case proposti.

Si prevede la predisposizione delle seguenti componenti:

- Una o più consolle Quest RMAD per la gestione del Disaster Recovery di tutte le foreste in perimetro, implementate su server con sistema operativo Windows Server;
- Una o più consolle Quest RMAD per la gestione degli eventi "day-by-day" di tutte le foreste AD in perimetro, implementate su server con sistema operativo Windows Server;
- Deploy di un numero di server da definire in fase di design, con sistema operativo Windows Server, da configurare come Secure Storage;
- Deploy di un numero di server da definire in fase di design, con le medesime caratteristiche HW e SW di ciascun DC che si intende proteggere, in join ai singoli domini AD in perimetro e da configurare con gli agent di recovery, per il ripristino dei DC a seguito di fault degli stessi.

Per quanto riguarda la gestione del backup di Active Directory (AD) il tool RMAD può gestirne il salvataggio sia internamente, tramite l'utilizzo del Secure Store Server, sia esternamente, su cloud storage Azure o AWS mediante integrazione nativa. È possibile anche combinare entrambe le modalità. La scelta dell'approccio più adatto verrà definita durante di installazione e configurazione.

5.2 SERVIZIO DI INSTALLAZIONE, CONFIGURAZIONE E MESSA IN ESERCIZIO

Il servizio in oggetto prevede, all'interno dell'attività di implementazione, le seguenti sei fasi:

- Startup di progetto: in particolare focalizzato sulla pianificazione esecutiva;
- Progettazione: disegno "high-level" dell'infrastruttura tecnologica basata su un singolo ambiente, integrato con tutte le foreste/domini in perimetro, in modo fornire una gestione centralizzata e che possa contenere l'impatto architetturale;

- Implementazione: predisposizione dell'infrastruttura per tutti i casi d'uso descritti all'interno del paragrafo precedente;
- Test del funzionamento in sandbox: esecuzione di test dell'infrastruttura RMAD per validare il corretto onboarding degli oggetti e degli scenari di recovery, in ambiente sandbox;
- Knowledge Transfer e Handover: preparazione di documentazione di progetto dettagliata e manuali che descrivono tecnologia implementata, processi, procedure e best practice, oltre all'affiancamento del personale IT del Cliente durante la fase di handover.

5.3 DELIVERABLE

I servizi di cui alla presente Capitolato sono da ritenersi completati nel momento in cui vengono consegnati a Consip i report con i risultati delle attività in oggetto, con relativo Verbale.

Tali deliverable saranno condivisi in un incontro congiunto fra il Fornitore e Consip.

L'accettazione dei deliverable è propedeutica al rilascio del positivo esito della verifica di conformità, il cui verbale rappresenterà la "Data di accettazione dei servizi".

5.4 SERVIZIO DI MANUTENZIONE

Oggetto del presente Capitolato è inoltre l'attivazione di un servizio specialistico erogato dal Fornitore pari alla durata del contratto, con lo scopo di supportare Consip nella gestione di *incident* relativi all'oggetto del presente Capitolato.

Fault / Incident Management : Il supporto prevede la presa in carico della chiamata, l'analisi e la gestione delle anomalie e fault derivanti da segnalazioni da parte del Cliente relative a malfunzionamenti rilevati sull'infrastruttura. E' prevista l'Apertura ticket di supporto al servizio Quest per ripristino delle funzionalità del tool a seguito di malfunzionamenti della piattaforma stessa.

Il Fornitore si obbliga a confermare al referente del Committente, secondo le modalità preventivamente concordate, l'avvenuta risoluzione del malfunzionamento.

5.5 SERVIZI PROFESSIONALI

Viene incluso nell'oggetto del contratto il servizio professionale a consumo per il supporto dei prodotti Software quantificati a 30 slot, per tutta la durata contrattuale.

6 LUOGO DI SVOLGIMENTO DEL SERVIZIO

Tutte le attività progettuali saranno svolte da remoto, ad eccezione della prima installazione del software di cui al punto 5.2 del presente Capitolato e di ulteriori incontri per lo svolgimento dei servizi professionali di cui al par. 5.5., su richiesta della Committente.

Le attività in presenza avverranno presso la sede Consip in Via Isonzo 19E, CAP 00198 Roma.

Resta inteso che eventuali costi di trasferimento e soggiorno del personale che svolge attività nell'ambito del presente Capitolato sono comunque a carico della Società.

7 RESPONSABILE DELLA FORNITURA

La Società dovrà comunicare, alla stipula del contratto, il nominativo del Responsabile della Fornitura, nonché un numero di telefono e un indirizzo e-mail al quale indirizzare eventuali comunicazioni.

Il Responsabile della fornitura sarà l'interlocutore unico della Committente per gli aspetti amministrativi, per l'organizzazione ed il coordinamento delle attività contrattuali.

8 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare, alla stipula del contratto, un indirizzo e-mail, un numero di telefono al quale rivolgersi, per ogni comunicazione relativa all'esecuzione delle attività contrattuali.

L'organizzazione del suddetto servizio di comunicazione dovrà essere a carico della Società.

Resta inteso che, per tutta la durata contrattuale, la Società dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicandone tempestivamente alla Committente le eventuali variazioni.

9 ADEMPIMENTI PER LA SICUREZZA

La Società aggiudicataria si impegna a porre in essere quanto necessario per garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D.Lgs. 81/2008 s.m.i., cooperando e coordinandosi, in particolare, con i referenti della Committente, ai fini degli adempimenti di cui all'art. 26 del citato decreto.

10 OBBLIGHI DI RISERVATEZZA

La Società si impegna ad adottare tutte le misure necessarie per garantire la massima riservatezza delle informazioni raccolte durante le attività descritte nel presente Capitolato Tecnico e a non divulgare, in nessun caso, a terzi i predetti dati, documenti, informazioni o parti di essi senza il preventivo ed esplicito accordo della Committente.

11 VERIFICA DI CONFORMITÀ

La verifica di conformità, di cui all'articolo 11 delle Condizioni Contrattuali, verrà eseguita al termine delle attività previste nel presente Capitolato Tecnico e sarà volta a certificare che le stesse siano state eseguite secondo le modalità indicate.

12 MODALITÀ DI FATTURAZIONE E PAGAMENTO

In relazione alle tipologie di servizio oggetto del presente Capitolato, le fatture dovranno essere prodotte secondo quanto disciplinato all'articolo 14 delle Condizioni contrattuali.

In particolare:

- relativamente ai servizi di cui ai Par. 5.1 e 5.2 ai fini del pagamento del corrispettivo indicato nel contratto, il Fornitore potrà emettere fattura, successivamente alla verifica di conformità emessa a seguito di deliverable di cui al par. 5.3 del presente Capitolato;
- relativamente al servizio di cui al Par. 5.4, ai fini del pagamento del corrispettivo indicato nel contratto, il Fornitore potrà emettere fattura con periodicità trimestrale posticipata riportata, successivamente alla relativa verifica di conformità positiva;
- relativamente al servizio di cui al Par. 5.5, ai fini del pagamento del corrispettivo indicato nel presente contratto, il Fornitore potrà emettere fattura con cadenza mensile, successivamente all'approvazione da parte della Committente del "consuntivo attività", contenente il dettaglio delle prestazioni erogate

nel periodo di riferimento, nonché della verifica di conformità positiva. Nella fattura dovrà essere indicato il periodo temporale di riferimento.

I termini di pagamento sono previsti a 30 giorni data ricevimento fattura.

13 LIVELLI DI SERVIZIO

Il Fornitore, nell'esecuzione del contratto, dovrà rispettare le seguenti scadenze e tutti i livelli di servizio di seguito indicati:

- il nominativo, i riferimenti telefonici e gli indirizzi email e PEC del **Responsabile della Fornitura** devono essere comunicati alla stipula del contratto;
- il **Piano di Lavoro** delle attività previste al Par. 5.2 del presente Capitolato deve essere consegnato entro 15 giorni lavorativi dalla stipula del contratto. Nel caso di richiesta da parte di Consip di modifiche, il nuovo Piano di Lavoro deve essere consegnato entro 5 (cinque) giorni lavorativi dalla richiesta di Consip;
- tutte le **scadenze riportate nel Piano di Lavoro** devono essere rispettate;
- l'**attivazione delle licenze per la fase di installazione e configurazione** deve avvenire entro i termini previsti dal Piano di lavoro;
- il **servizio di supporto professionale da remoto** deve essere garantito e disponibile dalle 8:00 alle 18:00 dal lunedì al venerdì, festivi esclusi;
- il **servizio di supporto professionale in presenza**, su richiesta di Consip, deve essere garantito entro 5 giorni lavorativi.

14 PENALI

La Committente, oltre a quanto previsto nelle Condizioni contrattuali, applicherà le penali, secondo le seguenti modalità:

1. per ogni giorno lavorativo di ritardo nella consegna del **Piano di Lavoro**, rispetto ai tempi previsti al precedente paragrafo 13 "Livelli di Servizio", Consip si riserva di applicare una penale pari all'uno per mille (1 ‰) dell'importo contrattuale;
2. per ogni giorno lavorativo di ritardo nella consegna dei **deliverable previsti dal Piano di Lavoro**, rispetto ai tempi ivi previsti, Consip si riserva di applicare una penale pari all'uno per mille (1 ‰) dell'importo contrattuale;
3. per ogni giorno lavorativo di ritardo nell'**attivazione delle licenze per la fase di installazione e configurazione**, rispetto ai tempi previsti dal Piano di Lavoro, Consip si riserva di applicare una penale pari all'uno per mille (1 ‰) dell'importo contrattuale;
4. per ogni evento di indisponibilità del **servizio di assistenza e supporto professionale**, rispetto alla disponibilità prevista al precedente paragrafo 13 "Livelli di Servizio", Consip si riserva di applicare una penale pari all'uno per mille (1 ‰) dell'importo contrattuale.