Piano per la sicurezza informatica

Il Comune di Zone si sta attualmente dotando di un piano per la sicurezza informatica, il disaster recovery e la continuità operativa aggiornati. Si allegano provvisoriamente l'ultima versione del documento programmatico per la sicurezza approvato (2008) e le linee guida per il disaster recovery e la continuità operativa (2012).

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

COMUNE DI

ZONE

2008

Approvato con deliberazione di G.C. n. 42 del 16.05.2008

Il presente documento è redatto sulla base delle "Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dagli articoli 34-35 e allegato B del D.Lgs. 196/03".

Indice

intentional blank page

Art. 31 - Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 32 - Particolari titolari

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

CAPO II - MISURE MINIME DI SICUREZZA

Art. 33 - Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34 - Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35 - Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36 - Adeguamento

Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

ALLEGATO B
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associa-

to a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per

la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'indi-

viduazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive

di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.
Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente

OBBIETTIVI DOCUMENTO

L'allegato B, punto 19 del D,Lgs. 196/03 impone la predisposizione e l'aggiornamento, con cadenza annuale, di un documento programmatico sulla sicurezza dei dati, per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare; la formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

L'articolazione progettuale del documento programmatico sulla sicurezza prevede le seguenti attività:

- Identificazione delle basi di dati
- Analisi del rischio
- Rassegna delle principali misure di controllo del rischio
- Definizione di misure di sicurezza fisiche, logiche ed organizzative, inclusi i siti di archiviazione dei dati, con particolare attenzione al controllo fisico e logico degli accessi
- Definizione di misure di sicurezza fisiche, logiche ed organizzative che assicurino l'integrità dei dati
- Definizione di misure di sicurezza fisiche, logiche e organizzative che garantiscono la sicurezza della trasmissione telematica dei dati
- Programma di formazione degli incaricati
- Piano di verifiche e di aggiornamento periodico del documento

Naturalmente la predisposizione di un tale piano richiede un'attenta analisi della situazione attuale del sistema informativo e di tutti i trattamenti di dati che vengono effettuati. Il presente documento rappresenta dunque una prima bozza che contiene alcune indicazioni sulla redazione del piano di sicurezza e che dovrà essere successivamente affinata al fine di ottenere un completo "manuale sulla sicurezza", anche in considerazione del fatto che nel Comune di ZONE è in fase di razionalizzazione e di ristrutturazione il Sistema Informativo, e che verrà completato nei prossimi mesi.

RUOLI E RESPONSABILITA'

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Comune di ZONE Via M. Guglielmo 42,
25050 Zone (BS) C.F. 80015590179 e P.Iva 00841790713
Telefono (segreteria) 030. .9870913; fax 030. .9880167;
e-mail: segreteria@comune.zone.bs.it

RESPONSABILI PER IL TRATTAMENTO DEI DATI PERSONALI

Segretario Comunale Protempore
Area Servizi Finanziari
Telefono 030.9870913;

Area Tecnica
Telefono 030.9870913;

AMMINISTRATORI DELLE PASSWORD E RESPONSABILI CED

Sig.ra Sina Anna
Telefono 030.9870913;

INDIVIDUAZIONE DELLE BANCHE DATI INFORMATIZZATE

1. Banca dati della popolazione residente
2. Banca dati degli elettori
3. Banca dati italiani residenti all'estero
4. Banca dati iscritti alla biblioteca comunale
5. Banca dati tributi comunali
6. Banca dati anagrafe tributaria
7. Banca dati catastale
8. Banca dati modello 730
9. Banca dati INPDAP
10. Banca dati modello 01/M
11. Banca dati inquadramento contrattuale
12. Banca dati buste paghe
13. Banca dati Delibere
14. Banca Dati Determine

INDIVIDUAZIONE DELLE BANCHE DATI CARTACEE[1]

1. Banca dati della popolazione residente
2. **Banca dati degli elettori**
3. Banca dati cittadini stranieri
4. Banca dati cessioni di fabbricato legge n 191/78
5. Banca dati leva militare
6. Banca dati iscritti alla biblioteca comunale
7. Banca dati servizi culturali-ricreativi-sportivi
8. Banca dati servizi pubblica istruzione
9. **Banca dati servizi socio-assistenziali**
10. Banca dati dei verbali di contestazione
11. Banca dati infrazioni al codice della strada
12. Banca dati tributi comunali
13. Banca dati dichiarazioni ICI
14. Banca dati TOSAP
15. Banca dati TARSU
16. Banca dati anagrafe tributaria
17. Banca dati catastale
18. **Banca dati titolari di autorizzazione al commercio fisso**
19. **Banca dati titolari pubblici esercizi**
20. **Banca dati commercio aree pubbliche**
21. **Banca dati dei dipendenti del Comune**
22. Banca dati rilevazione presenze del personale del Comune
23. Banca dati INPDAP
24. Banca dati modello 770
25. Banca dati modello 01/M
26. Banca dati inquadramento contrattuale
27. Banca dati degli incarichi professionali o stagionali del Comune
28. Banca dati degli amministratori del Comune
29. Banca dati degli insediamenti produttivi
30. **Banca dati ditte per gare d'appalto**
31. Banca dati concessioni edilizie
32. Banca dati condono edilizio
33. **Banca dati appaltatori servizi di manutenzione**
34. **Banca dati ditte e imprese partecipanti a gara ed esecutrici**
35. Banca Dati Urbanistica
36. Registro cartellini carta d'identità
37. Registro espatrio minori
38. Banca dati pratiche emigrazioni/immigrazioni
39. Banca dati trasferimenti interni
40. Banca dati assunzioni stranieri
41. **Banca dati tessera parcheggio invalidi**
42. Banca dati permessi di transito
43. Banca dati passi carrai
44. **Banca dati denuncia infortuni**
45. Banca dati protocollo del comune
46. Banca dati delle opere di congl. Cementizie
47. Banca dati pubbliche affissioni
48. Banca dati Risorse Boschive
49. Delibere
50. Determine
51. **Registro PG**

[1] In **ROSSO** i dati Giudiziari, in **GRIGIO** i dati Sensibili, in **BLU** i dati sia Sensibili che Giudiziari

INDIVIDUAZIONE DELLE BANCHE DATI TRATTATE ALL'ESTERNO

1. Banca dati Tarsu
2. Banca dati INPDAP
3. Banca dati modello 770
4. Banca dati degli elettori
5. Banca dati leva militare
6. Banca dati incarichi elettorali
7. Banca dati italiani residenti all'estero
8. Banca dati assunzioni stranieri
9. Schedario cartellini C.I.

Le banche dati numero 1,2 e 3 sono trattate da enti esterni i quali devono essere nominati come responsabili del trattamento.

Le restanti banche dati sono copie d'ufficio depositate presso altri enti per obbligo normativo.

INDIVIDUAZIONE DEI SETTORI E DEI RESPONSABILI

AREA CONTABILE AMMINISTRATIVA

Responsabile Almici Mario

- SERVIZIO SEGRETERIA
- SERVIZIO PERSONALE
- SERVIZIO CONTRATTI
- SERVIZIO ARCHIVIO
- SERVIZIO CULTURA
- SERVIZIO PUBBLICA ISTRUZIONE
- SERVIZIO SPORT
- SERVIZIO SOCIO-ASSISTENZIALE
- SERVIZIO BILANCIO E CONTABILITA'
- SERVIZIO ECONOMATO
- SERVIZIO TRIBUTI

AREA SERVIZI DEMOGRAFICI

Responsabile Marchetti Marco

- SERVIZIO ELETTORALE
- SERVIZIO DEMOGRAFICO
- SERVIZIO PROTOCOLLO

AREA TECNICA

Responsabile Segretario Comunale

- SERVIZIO URBANISTICA
- SERVIZIO EDILIZIA
- SERVIZIO LAVORI PUBBLICI E MANUTENZIONE
- SERVIZIO ECOLOGIA E AMBIENTE

AREA POLIZIA LOCALE

Responsabile Zatti Marco Antonio

- SERVIZIO PROTEZIONE CIVILE
- SERVIZIO POLIZIA LOCALE
- SERVIZIO COMMERCIO E ATTIVITA' PRODUTTIVE

INDIVIDUAZIONE UFFICIO DEGLI INCARICATI

Incaricato	**Ufficio**
Marchetti Marco	Anagrafe
Sina Anna	Tributi
Peli Giovanni	Biblioteca
Almici Mario	Segreteria
Almici Mario	Ragioneria
Almici Mario	Sociale
Zatti Marco Antonio	Polizia Locale
Segretario	Tecnico
Bettoni Sonia	Tecnico incaricato

INDIVIDUAZIONE DEGLI INCARICATI DEL TRATTAMENTO

Banche Dati	Incaricato/Incaricati
Banca dati della popolazione residente	Marchetti Marco; Almici Mario
Banca dati degli elettori.	Marchetti Marco; Almici Mario
Banca dati degli incarichi elettorali	Marchetti Marco; Almici Mario
Banca dati italiani residenti all'estero	Marchetti Marco; Almici Mario
Banca dati cittadini stranieri	Marchetti Marco; Almici Mario
Banca dati cessioni di fabbricato legge n. 191/78	Sina Anna; Zatti Marco
Banca dati leva militare	Marchetti Marco; Almici Mario
Banca dati iscritti alla biblioteca comunale	Peli Giovanni
Banca dati servizi culturali-ricreativi-sportivi	Almici Mario; Sina Anna
Banca dati servizi pubblica istruzione	Almici Mario; Sina Anna
Banca dati servizi socio-assistenziali	Almici Mario; Sina Anna
Banca dati dei passi carrai e permessi di transito	Zatti Marco
Banca dati dei verbali di contestazione	Zatti Marco
Banca dati infrazioni al codice della strada	Zatti Marco
Banca dati tributi comunali	Almici Mario; Sina Anna
Banca dati dichiarazioni ICI	Almici Mario; Sina Anna
Banca dati tarsu	Almici Mario; Sina Anna
Banca dati anagrafe tributaria	Almici Mario; Sina Anna; Segretario
Banca dati catastale	Segretario, Bettoni Sonia
Banca dati debitori	Almici Mario; Sina Anna
Banca dati creditori	Almici Mario; Sina Anna
Banca dati commercio aree pubbliche	Zatti Marco
Banca dati dei dipendenti del Comune	Almici Mario; Sina Anna
Banca dati rilevazione presenze del personale del Comune	Almici Mario; Sina Anna
Banca dati Risorse Boschive	Zatti Marco, Almici Mario
Banca dati INPDAP	Almici Mario; Sina Anna
Banca dati modello 770	Almici Mario; Sina Anna
Banca dati modello 01/M	Almici Mario; Sina Anna
Banca dati inquadramento contrattuale	Almici Mario; Sina Anna
Banca dati degli insediamenti produttivi	Segretario, Bettoni Sonia; Almici Mario
Banca dati concessioni edilizie	Segretario, Bettoni Sonia; Almici Mario
Banca dati condono edilizio	Segretario, Bettoni Sonia; Almici Mario
Banca dati urbanistica	Segretario, Bettoni Sonia; Almici Mario
Banca dati pratiche emigrazioni/immigrazioni	Marchetti Marco; Almici Mario
Banca dati assunzioni stranieri	Marchetti Marco; Zatti Marco
Banca dati denuncia infortuni	Marchetti Marco; Zatti Marco
Banca dati protocollo del comune	Marchetti Marco; Sina Anna
Banca dati TOSAP	Zatti Marco;Sina Anna
Banca dati titolari pubblici esercizi	Zatti Marco
Banca dati degli incarichi professionali o stagionali del Comune	Almici Mario; Sina Anna
Banca dati degli amministratori del Comune	Almici Mario; Sina Anna
Banca dati ditte per gare d'appalto	Almici Mario; Segretario, Bettoni Sonia
Banca dati appaltatori servizi di manutenzione	Almici Mario; Segretario, Bettoni Sonia
Banca dati ditte e imprese partecipanti a gara ed esecutrici	Almici Mario; Segretario, Bettoni Sonia
Registro cartellini carta d'identità	Marchetti Marco; Zatti Marco
Registro espatrio minori	Marchetti Marco; Almici Mario
Banca dati tessera parcheggio invalidi	Zatti Marco

ANALISI DEL RISCHIO

E' chiaro che non è possibile azzerare il livello di rischio, ma è importante valutare quale livello di rischio siamo disposti ad accettare.

Il maggior rischio che incombe sul sistema informativo comunale è chiaramente legato alla perdita dei dati con conseguente interruzione del servizio erogato. Il rischio è strettamente connesso al livello di sicurezza, sicurezza che oltre ad aspetti tecnologici è costruita sui buoni comportamenti degli utilizzatori, che contribuiscono ad alzarne il livello.

Questo modulo costituisce la fase di partenza delle attività di progettazione di un piano di sicurezza, e la sua predisposizione consente di:

- Acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo
- Creare una lista che identifica i possibili rischi (check list)
- Avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare
- Generare un elenco in ordine di priorità delle attività da implementare per ridurre il rischio

COMUNITA' MONTANA & COMUNE DI ZONE[2]

Poiché la C.M. è interessata alla gestione parziale del SIC, integro in questo documento le risposte del loro responsabile, sig. Nicola Riolini, sotto forma di e-mail:

Da: sergio.pellanda@aliceposta.it]
Inviato: lunedì 29 novembre 2004 18.49
A: riolini@micronaet.it
Oggetto: Comune di Zone - DPS

Il comune di Zone mi ha dato l'incarico di stendere il Documento Programmatico sulla Sicurezza (Dlgs 196/03). Il signor Almici mi ha detto di rivolgermi a lei per alcune problematiche a cui lui non sapeva rispondere.
Premesso che io non conosco il tipo di lavoro che lei (per la Comunità Montana) svolge sul comune di Zone, alcune domande che le faccio potrebbero essere fuori contesto. Se mi fa sapere quale tipo di contratto c'è tra Voi (Comunità Montana) e il Comune posso anche capire a quali servizi fornite assistenza.
Intanto le domande sono queste:

1) Quali software (eccetto Delisa) sono forniti di licenza (SO, Office, ecc...)? E quante licenze ci sono? E dove sono?
2) L'antivirus è gestito da Voi? Come è impostato l'AV?
3) Esiste un contratto di assistenza HW/SW sul Server? C'è solo la garanzia? E' scaduta? Siete voi ad occuparvene?
4) Esiste un contratto di assistenza HW/SW sui client? ecc...
5) Esiste un contrattop di assistenza sulle stampanti?ecc...
6) Chi si occupa del backup, esclusa la sostituzione delle cassette?
7) Nel caso in cui il server si guastasse, chi si occupa della procedura di recovery?
8) Nel caso in cui un Client si guastasse, chi si occupa del ripristino?
9) Esiste un firewall tra la LAN e Internet? La procedura di accesso è tramite account? E' attivo un log? C'è un proxy?

Spero di aver esaurito le domande, ma in base alle sue risposte è possibile che debba fargliene altre.
La ringrazio anticipatamente per il tempo che mi dedica.
Sergio Pellanda

La risposta è stata:

Io sono responsabile per la Comunità Montana del sistema SIS ovvero della interconnessione dei vari Comuni ai server centrali della C.M.
Amministro e mantengo i server dislocati presso i Comuni che ne fanno parte e rispondo in prima battuta dei problemi che possono nascere in merito al programma di protocollo, dell'accesso ad internet (in merito alla mancata disponibilità della connessione), dell'installazione antivirus (dove mi viene indicato e da quasi sempre da remoto), degli eventuali problemi tecnici riguardo lo sportello unico, e per problemi generici sempre legati alla rete SIS.
Cercherò per quanto mi è disponibile rispondere alle sue domande:

1. I software forniti dalla C.M. sono Optix (licenza cumulativa), NAV CE (licenza cumulativa in C.M.), per le postazioni direttamente fornite Windows 2000 e Office SBE (non avendo fatto io l'installazione non sono in grado di dirvi se sono state consegnate o sono presenti in C.M.)
2. L'antivirus è gestito da noi e controlliamo settimanalmente gli aggiornamenti e le postazioni con rilevamenti virus. Il fine è quello di controllare che i virus rilevati non abbiano intaccato il sistema (sempre dove possiamo effettuare l'amministrazione remota, ovvero nei PC direttamente rilasciati dalla C.M. o in quelli installati secondo le nostre specifiche). La protezione è attiva e l'aggiornamento è automatico.
3. Il server ha un contratto di assistenza rinnovato quest'anno da me al termine dei 3 anni di garanzia per un altro anno (chiedere in C.M. l'eventuale scadenza corretta). La garanzia è sulle parti HW, in seguito a guasti che portano alla reinstallazione è intervenuta la C.M., come in passato.
4. Abbiamo fatto presente della scadenza della garanzia e dato la disponibilità per intercedere con la ditta utilizzata dalla C.M. per l'estensione (cercando di spuntare una tariffa agevolata) ma non abbiamo avuto riscontri dal Comune.
5. Come sopra
6. Il backup viene controllato settimanalmente dalla C.M. ed eventuali malfunzionamenti sono segnalati alla IBM, i dati però inseriti nel backup sono quelli del programma Optix (fatto in C.M.), quelli di eventuali programmi con dati sul server (Delisa, che tra l'altro hanno una loro procedura autonoma di cui non sono stato informato) e, come spesse volte ricordato, i files presenti effettivamente sul server (premesso che, essendoci stati nuovi inserimenti di personal computer non coordinati da noi, non ho idea di che tipologie di dato potrebbero essere dislocate su client di rete)
7. In seguito a guasti HW e a ripristino dovuto a problemi effettivamente attribuibili a guasto imprevedibile, interverrebbe la Comunità Montana (come è successo in passato) in caso a guasti causati da installazioni di terzi che destabilizzano il sistema operativo, incuria o mancata manutenzione da parte del Comune (UPS non collegato, urti o quant'altro)
8. Il ripristino del client ci riguarda solo a PC reinstallato per i software da noi gestiti sempre previo l'installazione di un client VNC per l'amministrazione remota (per evitare spostamenti e dispendio di tempo per gli stessi)
9. Il firewall esiste ma è in via di sostituzione con l'anno prossimo, l'idea è quella di acquistare un firewall proxy con log e blocco ai siti ludici. L'autenticazione sarà come quella attuale con password e nome utente. L'accesso ad internet passa attraverso la rete Comunale uscendo dalla C.M. con una HDSL a 2 Mbit, spero che il Comune non utilizzi modem o altre apparecchiature per accessi autonomi ad internet.

Cordiali saluti
Nicola Riolini

Mi pare di capire che esiste un coinvolgimento solo parziale della C.M. nella gestione e manutenzione del sistema informativo comunale. Dalla e-mail, si capisce che tale gestione è limitata ad alcuni oggetti (hardware o software), e che, nell'impostazione e gestione del Server, ci sia anche l'intervento di altre persone (ad esempio tecnici Delisa). Sarebbe meglio evitare questa prassi. Pertanto, io consiglio all'amministrazione del comune di Zone di chiarire, ed eventualmente allargare, il contratto con la C.M., in modo da estenderlo:

- alla manutenzione dei client, anche non acquistati direttamente da loro
- alla manutenzione dell'altro hardware presente nei locali (printer, ecc…)
- alla manutenzione del software (non Delisa) utilizzato (es. Office SBS)
- al controllo della procedura di Backup e Restore dell'intero SIC e non di una sola sua parte.

In questo modo, il comune, avrà una sola interfaccia per gestire al meglio le risorse interne (PC, printer, router, server, ecc…), senza incorrere nello spiacevole atteggiamento di "scarica barile" a cui si presta un sistema amministrato da più persone.

[2] Dal 31/1/2007 la comunità montana non fornisce i servizi in elenco nella pagina; sono rimasti alcuni retaggi come l'Antivirus.

TABELLA DEI RISCHI

	Descrizione Rischio	*IMPATTO SULLA SICUREZZA*
Strumentali	Intercettazione dati	BASSO, è attivo un firewall e non si deve installare software non certificato dal CED
	Interruzione alimentazione	NULLO, il server è sotto UPS
		MEDIO, i PC non sono protetti da UPS
	Virus e affini	BASSO, antivirus attivo e aggiornato
	Blocco Sistema	BASSO, i PC sono in LAN e quindi intercambiabili
		MEDIO, il server non è sostituibile
	Accesso non autorizzato	MEDIO, la procedura di autenticazione è di per sé debole
	Sabotaggio	BASSO, il comune non è un obiettivo sensibile
	Malfunzionamento HW Malfunzionamento SW	BASSO, il Personal Computer ha poca valenza
		MEDIO, il Server è sempre acceso e vitale per il funzionamento
Operatori	Carenza di consapevolezza	BASSO, il personale è discretamente addestrato
	Sottrazione credenziali	ALTO, esiste la prassi di comunicare ai colleghi le proprie credenziali
	Errori digitazione	BASSO, il personale è discretamente addestrato
	Comportamento fraudolento	BASSO, i dati trattati non sono di particolare interesse ne informativo ne economico
Contestuali	Accesso ai locali Sottrazione di strumenti con dati	MEDIA, la struttura non è dotata di impianto di allarme o porte blindate
	Catastrofi	MEDIA, copia dei dati non è conservata in luoghi diversi dai dati stessi, ne riposti in cassaforte ignifuga
	Errori umani sulla sicurezza fisica	BASSA, il personale è discretamente addestrato

CONTROMISURE ESISTENTI E DA ADOTTARE

Da adottare	Esistente
a. Eseguire sempre la valutazione preventiva del nuovo software[3], o installare solo software certificato. b. Acquistare eventuali licenze mancanti (verificare il numero di licenze). c. Impostare il sistema in modo da forzare l'utente a: – *Cambiare la password periodicamente, con una frequenza non superiore a sei mesi* – *A imporre alla password la lunghezza minima pari a 8 caratteri* – *A non poter riutilizzare la stessa password* d. Filtrare la posta con antispam. e. Archiviare la documentazione cartacea contenente dati **giudiziari** in armadi dotati di serratura la cui chiave è a disposizione unicamente degli incaricati che ne curano la chiusura dopo ogni utilizzo limitando tali operazioni a quelle strettamente necessarie allo svolgimento dei compiti d'ufficio. f. Archiviare la documentazione cartacea relativa ai dati **sensibili** in armadi dotati di serratura la cui chiave è a disposizione unicamente degli incaricati che ne curano la chiusura dopo ogni utilizzo limitando tali operazioni a quelle strettamente necessarie allo svolgimento dei compiti d'ufficio. g. Proteggere i dati sensibili, fatti di documenti Word ed Excel, tramite password in lettura/scrittura e renderli accessibili in rete solo all'incaricato, dove possibile usare EFS (Encrypting File System). h. Incaricare del trattamento gli enti esterni, tramite lettera. i. Consentire l'accesso al sistema informatico solo agli operatori con credenziali o ad eventuali tecnici manutentori. Questo, in parte è gia attivo[4], ma l'uso di credenziali biometriche o smart card renderebbe molto più efficace la protezione. l. Usare le chiavi degli armadi e delle porte disponibili. m. Acquistare Software antivirus poiché la Comunità Montana non gestisce più gli aggiornamenti.	1.Accesso limitato al server (armadio) ai soli addetti al CED o alle persone espressamente autorizzate dagli stessi, per il tempo strettamente necessario allo svolgimento dei compiti eventualmente assegnati. 2.Esecuzione automatica del backup giornaliero. 3.Tutti i PC aggiornati a Windows 2000 o sup. 4.Tutto il software installato solo da supporti fisici dei quali è nota la provenienza. 5. Gruppo di continuità generale. 6. Protezione delle risorse attraverso autorizzazione. 7. Spostato in cassaforte l'archivio dei nastri e le licenze software.

[3] Per nuovo software non intendo gli aggiornamenti.

[4] Gli operatori devono inserire nome utente e password per accedere al sistema, ma questo non ha impedito di far circolare le proprie credenziali di accesso.

INDIVIDUAZIONE DELLE MISURE MINIME IN ATTO E DA ATTUARE

L'allegato B al D.Lgs. 196/03[5] indica quali sono le misure minime da adottare al 31/06/2005. Nella prima colonna tabella sono riportati tutti gli articoli del disciplinare tecnico; l'altra colonna riporta lo stato: "in atto" o "da attuare" del SIC in analisi.

Sistema di autenticazione informatica

Come gia riferito il sistema di autenticazione è impostato per richiedere le credenziali di accesso (nomeutente+password). Questo protezione non ha avuto, a mio giudizio, l'impatto adeguato di sicurezza a causa della scarsa segretezza che mantengono tali credenziali. Nei punti che seguono mi riferisco comunque a questo sistema come mezzo di autenticazione, anche se risulta altamente vulnerabile.

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.	**In atto**
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.	**In atto**
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.	**In atto**
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.	**In atto**
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.	**In atto**
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.	**In atto**
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.	**In atto**
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.	**In atto**
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.	**In atto**
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.	**In atto**
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.	**Ovvio**

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.	**In atto**
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.	**In atto**
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	**Da attuare**

[5] Cfr pag 4

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.	**Da attuare**
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.	**Da attuare**
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.	**Da attuare**
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.	**In atto**

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:	**In atto**
19.1. l'elenco dei trattamenti di dati personali;	**In atto**
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;	**In atto**
19.3. l'analisi dei rischi che incombono sui dati;	**In atto**
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;	**In atto**
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;	**In atto**
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;	**In atto**
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;	**In atto**
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.	**In atto**

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.	**Non ci sono dati sensibili o giudiziari informatizzati**
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.	
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.	
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.	
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.	**Non interessa gli enti comunali**

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.	**Da attuare**
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.	**Da attuare**

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.	**In atto**
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.	**In atto**
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente	**In atto**

CONTROMISURE E AZIONI DA ADOTTARE IN ORDINE DI PRIORITA'

A mio avviso, l'amministrazione del comune di Zone dovrebbe rendere operative le seguenti contromisure e azioni in ordine di priorità:

1. **acquistare un software antivirus e sottoscrivere il sevizio di aggiornamento;**
2. **acquistare un NAS *(Network Attached Storage*) un disco di rete (>250Gb) aggiuntivo per tenere una copia solo dei dati (~150€);**
3. sostituire eventuali PC datati e con S.O. non adatto (Windows 9x);
4. attivare il sistema di credenziali minimo richiesto;
5. impostare la disconnessione (logoff) automatica dopo 15 minuti di inutilizzo;
6. incaricare del trattamento, in forma scritta, tutto il personale coinvolto;
7. incaricare del trattamento, in forma scritta, gli enti esterni;
8. incaricare gli addetti ai vari servizi;
9. prevedere corsi di formazione per illustrare il decreto 196/03;
10. prevedere corsi di formazione per addestrare gli operatori ad un uso appropriato del PC;

MODALITA' DI RIPRISTINO DATI

Tale procedura è nota con il termine **Disaster Recovery** e deve elencare le modalità da seguire per ripristinare l'intero SIC del comune nonché i tempi massimi previsti per la suddetta procedura.

Definizione
Per Disaster Recovery si intende l'insieme di misure tecnologiche e processi organizzativi atti a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze.

Emergenza: Disastro totale della sala server, con il Domain Controller fuori uso.

Preliminarmente viene preparata una postazione (pc ibm compatibile o un nuovo server completo di video e tastiera) e viene installato il software Windows 2003 Server Standard Edition in dotazione al Comune.

Checklist

- Il cd originale windows 2k3 utilizzato nella precedente installazione e il key-code
- un account amministrativo valido nel dominio
- il backup del system state non più vecchio di 60 giorni
- la copia dei dati
- un collegamento ad internet

Il processo di bootstrap deve essere eseguito da CD (impostazione normalmente predefinita) e preliminarmente deve essere alloggiato nell'apposito contenitore il cd-rom Windows 2003 Server.

Installazione windows 2003 standalone <obbligatorio>

1) Alla domanda "Premere un tasto per avviare da cd" , premerlo. Nel caso l'avvio non avvenga da cd, entrare nel bios e modificare l'ordine di avvio, mettendo al primo posto il cd.
2) Finestra Installazione di Windows Server, premere invio per installare.
3) Premere F8 per accettare il contratto;
4) Premere D per eliminare eventuali partizioni presenti;
5) Premere Invio per continuare;
6) Premere L per confermare l'eliminazione;
7) Premere C per creare una nuova partizione e stabilire la dimensione della partizione (minimo 10 giga);
8) Premere Invio due volte;
9) Scegliere l'opzione "Formattare la partizione usando il file system NTFS e attendere;
10) Il computer si riavvia al termine della prima fase dell'installazione, non premere nessun tasto e attendere il completamento dell'installazione (circa 40 minuti);
11) Opzioni internazionali e della lingua avanti;
12) Digitare nome utente e Organizzazione: digitare Comune di Zone in entrambi i campi;
13) Digitare il product key, quindi avanti;
14) Selezionare la modalità di gestione licenze: Per dispositivo o per Utente, avanti;
15) Nome Computer ***Srvzone***, non digitare la password per il momento, quindi avanti;
16) Impostazioni data e ora, controllare ora e data e premere avanti;
17) Impostazioni di rete: scegliere impostazioni personalizzate, avanti;
18) Componenti di rete: selezionare Protocollo Internet TCP/IP, proprietà, selezionare utilizza il seguente indirizzo IP, digitare per IP: 192.168.206.2, per subnet mask: 255.255.255.0, per ga-

teway: 192.168.206.254, Selezionare a questo punto Utilizza i seguenti indirizzi DNS e scrivere al valore predefinito: 151.99.125.2 e l'alternativo lasciarlo vuoto;Premere OK., quindi avanti;

19) Gruppo di lavoro o dominio del computer: Scegliere NO, questo computer non è in rete.., avanti;
20) Il computer si riavvia per la seconda volta, a questo punto il sistema operativo è installato e, quindi, si accede al software con i tasti CTR+ALT+CANC, quindi INVIO;

Installazione SERVICEPACK 1 del server da ripristinare. <obbligatorio>

21) Collegarsi al sito windows update o Inserire il CD contenente il service pack1 ed eseguirlo, attendere l'installazione e riavviare. Installare anche le PATCH più importanti (da sito microsoft [meglio] o da CD);
22) Nel caso non si possieda il CD verificare il collegamento alla rete aziendale (ping 192.168.206.254) e verificare il collegamento ad internet (iexplorer);

Promuovere a Domain Controller con DNS.

23) Entrare, inserire CD windows 2003 server
24) Cliccare su start → esegui, digitare dcpromo
25) Avanti, avanti
    a. Tipo di controller di dominio, selezionare controller di dominio di un nuovo dominio;
    a. Crea Nuovo dominio in un nuovo insieme di strutture, avanti;
    b. Nome DNS del nuovo dominio: zone.locale, avanti;
    c. Nome dominio netBIOS: **ZONE**, avanti;
    d. Cartelle dei database e dei registri, non modificare, avanti;
    e. Volume di sistema condiviso, non modificare, avanti;
    f. Diagnostica registrazione DNS: Assicurarsi che sia selezionata la voce: "Installa e configura il server DNS su questo computer…", avanti;
    g. Autorizzazioni: Selezionare la voce "Autorizzazioni compatibili soltanto con SO Windows 2000 o superiori", avanti;
    h. Password di Amministratore, modalità ripristino servizi, lasciare tutto vuoto, avanti, avanti
26) Dopo l'installazione spegnere il PC.

Ripristino System State

(il backup del system state non deve essere più vecchio di 60 giorni e l'hardware dovrebbe essere quello da cui è stato fatto il backup, il ripristino si può tentare anche su altro hw)

27) Riavviare il computer.
28) Premere il tasto F8 per entrare nel menu opzioni avanzate di Windows.
29) Selezionare **modalità ripristino servizi directory (solo controller dominio windows)**, invio.
30) Selezionare S.O. da avviare, invio.
31) Accedere al sistema nel modo tradizionale.
32) Inserire cd contenente il backup più recente del system state.
33) Avviare NTBACKUP: start , esegui, digitare ntbackup, ok.
34) Deselezionare avvio guidato., avanti.
35) Selezionare ripristino dei file, avanti.
36) Sfoglia e selezionare il backup del system state posto sul cd.
37) Doppio clic (finestra lato destro) sul nome del set di backup per eseguire l'inventario.
38) Sul lato sinistro (elementi da ripritinare) compare backup system state, selezionare la voce system state , avanti.
39) Selezionare avanzate, selezionare percorso originale, lanciare il ripristino, ok., ok.
40) Dopo il ripristino accettare il riavvio del computer **in modalità provvisoria**
41) Premere il tasto F8 per entrare nel menu opzioni avanzate di Windows.
42) Selezionare **modalità provvisoria**

43) Digitare l'account amministrativo che si usava in precedenza (administrator, *passwordvalida*)
44) Lasciare che il Sistema rilevi nuovamente tutte le periferiche
45) Riavviare

Procedura di attivazione del software Windows2003 (obbligatoria)
(è necessario un collegamento internet verso microsoft.com)
46) Digitare un account amministrativo valido nel dominio
47) Seguire le istruzioni a video

A questo punto il server dovrebbe essere configurato con utenti e PC presenti nel dominio, ma senza dati.

Tempo 4/5h senza inconvenienti.

A questo punto devono essere re-installate e ripristinate le applicazioni del Sistema Informativo Comunale (es. applicazioni Delisa, ecc…) e i Dati degli utenti (es. documenti word, ecc…).

FORMAZIONE

La formazione è una fase obbligatoria e la messa in atto di tale processo diretto ad approfondire il D.Lgs. n. 196/03 è a discrezione dell'amministrazione comunale che individua tempi e modalità per coinvolgere i dipendenti nell'attuazione del decreto.
La formazione del personale per l'uso appropriato e adeguato dei mezzi e degli strumenti (antivirus, posta, password, ecc…) da utilizzare, sarà interna e a rotazione. Alcuni dipendenti saranno addestrati e sensibilizzati sulle procedure in caso di virus, cambio password, gestione posta elettronica, cartelle condivise, crittografia per dati sensibili, inoltre saranno date "*istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento*".
Prevedo che la formazione durerà circa 2/3 ore per turno e terminerà con la consegna di un memorandum (predisposto dall'ufficio competente) sugli atteggiamenti corretti da adottare in caso di crisi.

VERIFICHE E AGGIORNAMENTI

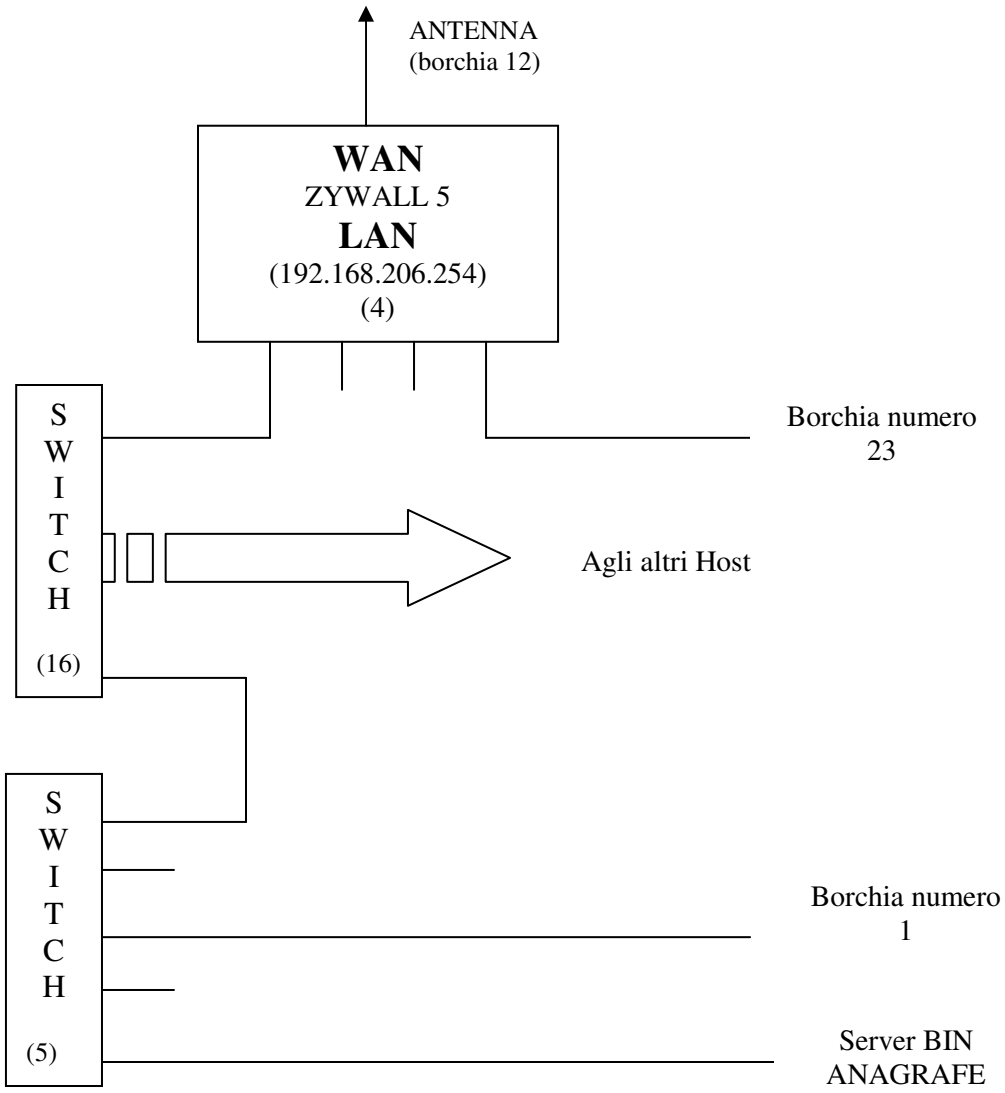
Perché il piano di sicurezza possa essere realmente efficace, deve essere verificato periodicamente. Il test delle singole misure e del piano nel suo complesso è un aspetto essenziale ed è l'unico strumento che conferisce al piano una credibilità.
Pertanto tutte le aree di rischio e tutte le contromisure adottate devono essere ciclicamente verificate con tecniche e procedure che non lascino dubbi sulla completezza e credibilità del test.
In particolare, quindi, dovranno essere effettuati, almeno annualmente, test relativi a:

- *Accesso fisico ai locali dove si svolgono trattamenti manuali e autorizzati.*
- *Gestione di codici identificativi personali e password.*
- *Gestione dei profili di accesso degli incaricati.*
- *Procedure atte a verificare l'integrità: Antivirus aggiornato.*
- *Sicurezza delle trasmissioni in rete: firewall testato.*
- *Modalità di conservazione dei documenti cartacei.*
- *Modalità di conservazione dei backup.*
- *Livello di formazione e grado di apprendimento degli incaricati.*

Il presente documento dovrà essere inoltre rivisto ed aggiornato almeno annualmente e comunque ogni qualvolta si apportino variazioni al sistema informativo, alle strutture o a qualunque altro elemento individuato dal piano o, se ne dovesse ravvisare l'opportunità e/o la necessità, in dipendenza di eventi non considerati dal presente programma.

IDENTIFICAZIONE STRUTTURA INFORMATICA

Ufficio	Utente	PC	Ip	SO
anagrafe elettorale	Marchetti Marco	Marchetti	192.168.206.50	w2kp
Anagrafe Ina saia	Marchetti Marco	Zone-anagrafe1	192.168.206.98	wxp
ragioneria	Almici Mario	Almici	192.168.206.13	w2kp
tributi	Sina Anna	pcanna	192.168.206.108	wxp
biblioteca	Peli Giovanni	Bibliote-18aufg	192.168.206.32	w2kp
protocollo	Marchetti/Sina	Protocollo	192.168.206.105	wxp
vigile	Zatti Marco	Sina	192.168.206.91	wxp
tecnico	tecnico	pctecnico	192.168.206.111	wxp
segretario	Segretario	Tecnico2	192.168.206.167	wxp
amministratori		Gis	192.168.200.104	wvista
ced		Srzone	192.168.206.2	w2k3srv
hp5000			192.168.206.99	
Canon3570			192.168.206.223	
Router (Zywall 5)	Paswd:	**Linkem**	192.168.206.254	


ANTENNA
(borchia 12)
WAN
ZYWALL 5
LAN
(192.168.206.254)
(4)
S
W
I
T
C
H
(16)
Borchia numero
23
Agli altri Host
S
W
I
T
C
H
(5)
Borchia numero
1
Server BIN
ANAGRAFE

Facsimile di lettera da inviare ad ogni utente

Comune di Zone Via Monte Guglielmo n. 42
25050 Zone (BS) C.F.: 80015590179 P.Iva 00841790173
Telefono (segreteria) 030.9870913; fax 030.9880167;
e-mail: segreteria@comune.zone.bs.it

_____, *lì* _____

Al Direttore Generale
Ai Funzionari
Ai Responsabili d'Ufficio
e.p.c. *Al personale operante con il SIC*
LORO SEDI

La sempre più crescente diffusione di personal computer, nonché l'entrata in vigore del D.Lgs. 196/03 impongono una più razionale e soprattutto sicura gestione degli accessi al database comunale.
È necessario, quindi, che tutti gli utenti, attuali e futuri, si attengano alle disposizioni qui di seguito elencate ed è compito dei responsabili di area fare in modo che le disposizioni siano rispettate dai propri collaboratori.

Nuove disposizioni sugli accessi al database comunale

Il CED provvederà a cambiare la periodicità della validità delle parole chiave di accesso al sistema informativo comunale (PASSWORDS).
Queste avranno validità **180 giorni,** passati i quali l'utente dovrà utilizzare una **NUOVA PASSWORD**.
Alla scadenza del periodo di validità, gli utenti saranno informati automaticamente da un messaggio inviato dall'elaboratore che la propria password è in scadenza e che è necessario immetterne una nuova.

Il nome utente è costituito dal cognome.:

UTENTE ANAGRAFE: BIANCHI MARIO

USER: BIANCHI

PASSWORD: qwSe12rt1*)

i caratteri possibili sono: [a-z], [A-Z], [0-9] [£ $ % & ( ) [ ] { } ^ *] evitare i caratteri di punteggiatura

I tentativi di accesso al S.I.C. saranno limitati a tre (3): gli utenti che digiteranno la propria password in modo errato e ripeteranno in successione l'errore altre due (2) volte, saranno automaticamente disabilitati e quindi verrà loro revocata la possibilità di accedere al SIC.

Nota: In questi casi, l'utente disabilitato dovrà comunicare al CED l'inconveniente operativo: verrà nuovamente reso operativo attraverso le procedure di sicurezza per le quali è abilitato esclusivamente il CED.

Sarà attivato il "time-out" di sistema: ciò significa che i lavori presenti nel sistema, ma inattivi, saranno disconnessi dopo 30 minuti. In pratica non sarà più possibile allontanarsi dal proprio "terminale" con videate aperte: trascorsi 30 minuti il sistema provvederà a disconnettersi automaticamente.
Va comunque ricordato che è **obbligatorio** durante le pause operative (intervallo per il pranzo) chiudere la propria sessione di lavoro e tornare sul menù d'inizio lavoro (**n.b.** il menù che richiede l'inserimento della password).
Infine si ricorda che le passwords una volta inserite, avranno validità **180 giorni** e che non potranno più essere riutilizzate.

CONCLUSIONI

Come premesso, le regole sopra citate sono volte a migliorare e garantire la sicurezza degli accessi al SIC, pertanto si raccomandano i signori utenti a coglierne significati e scopi.
Inoltre è **VIETATO** comunicare ai colleghi la propria password di accesso al SIC: **questa prassi non è PERMESSA**, anche nel caso in cui l'utilizzo della password del collega è giustificata dal fatto che una funzione procedurale non è presente sul proprio menù, ma su quello del collega stesso. L'utente sprovvisto della funzione interessata dovrà farne richiesta al proprio responsabile e questi direttamente al personale CED.

Qualsiasi variazione riguardate l'abilitazione all'uso dei personal computer dovrà pervenire al CED in forma scritta con l'autorizzazione del Funzionario di settore.

Le nuove disposizioni entreranno in vigore il 1 Gennaio 2005.

Il responsabile del procedimento

Agenzia per l'Italia Digitale

I SERVIZI MINIMI ESSENZIALI PER L'ADOZIONE DELLE SOLUZIONI DI DISASTER RECOVERY, IN LINEA CON L'ART. 50-BIS DEL CAD

VERSIONE 2.4 DEL 30/07/2012

SOMMARIO

1. Introduzione

Il Codice dell'Amministrazione Digitale, il D.lgs. n. 82/2005 e s.m.i. (aggiornato in particolare dal D.lgs. n. 235/20120, nel prosieguo per brevità chiamato CAD), sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la digitalizzazione dei servizi ICT (art. 15 "*Digitalizzazione e riorganizzazione").*
Da tale indicazione consegue per la Pubblica Amministrazione anche l'obbligo di assicurare la continuità dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese. Questa affermazione assume particolare significato a fronte del sempre maggiore utilizzo delle tecnologie ICT per la gestione dei dati e dei processi interni ai singoli enti, il cui impiego deve essere realizzato anche pianificando le necessarie iniziative tese a salvaguardare l'integrità, la disponibilità, la continuità nella fruibilità delle informazioni stesse. Quando i dati, le informazioni e le applicazioni che li trattano sono parte essenziale ed indispensabile per lo svolgimento delle funzioni istituzionali di un ente/organizzazione, diventano un bene primario cui è necessario garantire salvaguardia e disponibilità, anche attraverso l'adozione di misure di sicurezza e di continuità operativa, in modo da garantire la continuità di funzionamento dei sistemi informativi.
In particolare l'articolo 50-bis del CAD ("*Continuità operativa")* delinea gli obblighi, gli adempimenti e i compiti che spettano alle Pubbliche Amministrazioni, a DigitPA (ora Agenzia per l'Italia Digitale) e al Ministro competente, ai fini dell'attuazione della continuità operativa e delle indispensabili soluzioni di Disaster Recovery, richiedendo che le Pubbliche Amministrazione definiscano i piani di continuità operativa e "s*ulla base di appositi e dettagliati studi di fattibilità tecnica"* [per i quali] "*è obbligatoriamente acquisito il parere di DigitPA."*

Per supportare le Amministrazioni nell'attuazione degli adempimenti previsti dal citato art. 50 bis. l'allora DigitPA ha provveduto ad emanare le "Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni" e la relativa Circolare del 1 dicembre 2011, n. 58, mettendo, inoltre, a disposizione delle Amministrazioni un apposito strumento di autovalutazione come ausilio nella valutazione della critcità dei servizi e nell'individuazione delle soluzioni tecniche.
Si è altresì ritenuto opportuno istituire un tavolo tecnico che riunisse le varie competenze professionali e del mercato, unitamente a quelle delle PP.AA., per individuare i servizi minimi essenziali per l'adozione delle soluzioni di Disaster Recovery, facilitando quindi il rapporto tra Amministrazioni e fornitori.

2. Scopo del documento

Scopo del presente documento e' quello di evidenziare i servizi minimi essenziali per le soluzioni di DR.
Il documento, che non intende elencare tutte le forniture e servizi informatici che si possono reperire sul mercato, né intende essere esaustivo in merito alle possibili combinazioni che si possono adottare, definisce delle "schede di servizio" che possono essere utilizzate da tutte le pubbliche amministrazioni sia centrali, sia locali, per rivolgersi ai fornitori, al fine di richiedere i servizi necessari per dotarsi di soluzioni di Disaster Recovery o anche per migliorare quelle esistenti.

Le schede, che descrivono i servizi minimi essenziali e i loro relativi sottoservizi, possono essere riassunte come segue:

LISTA SERVIZI	BREVE DESCRIZIONE E SOTTOSERVIZI
D1: Supporto alla predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4, dell'art. 50-bis del CAD.	Servizi di consulenza e supporto alla redazione della documentazione necessaria alla richiesta di parere. Sottoservizi: A.Supporto per: -la compilazione delle schede di autovalutazione; -la predisposizione dello Studio di Fattibilità Tecnica; -la predisposizione della Relazione Tecnica sullo stato di attuazione del CAD. B. Consulenza per Business Impact Analisys (BIA): Individuazione e valutazione servizi critici per la sopravvivenza del business; C.Consulenza per Risk Assessment (RA): Valutazione
D2 -Servizio di Predisposizione dei piani di CO/DR e di progettazione organizzativa/procedurale e tecnologica della soluzione di DR"	Il servizio attiene alla produzione del piano di continuità operativa e di disaster recovery (CO/DR) partendo dallo studio di fattibilità (predisposto con la scheda D1) Sottoservizi: A. Progettazione di alto livello del modello organizzativo B. Progettazione di alto livello della soluzione tecnologica, con eventuale produzione di deliverable/studi per il consolidamento o la razionalizzazione del SI Primario (ove se ne evidenzi la necessità come passo propedeutico/prerequisito ai fini della realizzazione della soluzione di DR) C.Progettazione di dettaglio del modello organizzativo/procedurale D.Progettaz. di dettaglio della soluzione tecnologica E. Redazione delle procedure di DR F. Redazione del piano di CO
D3: Il sito di DR: aree CED e aree attrezzate per posti di lavoro	Disponibilità e mantenimento di aree CED e aree per PdL, nel quale siano installati o installabili i sistemi necessari a ripristinare i servizi informatici identificati nello Studio di Fattibilità e dettagliati nel progetto esecutivo. Il servizio potrà articolarsi nei seguenti sotto-servizi: A. Disponibilità della struttura edile e impiantistica per gli spazi del sito di DR B. Esecuzione degli eventuali interventi sul sito primario e sul sito di DR comprensiva, ove necessario, della predisposizione dell'infrastruttura tecnico-logistica, per renderlo conforme ai requisiti minimi obbligatori riportati in allegato alla presente scheda D3, definiti – a seguito dei servizi di progettazione della scheda D2 – come passo propedeutico/prerequisito della realizzazione della soluzione di DR C. Gestione e manutenzione del sito di DR D. Disponibilità di spazi ad uso ufficio destinati ad ospitare le PdL secondo le modalità descritte nella scheda D4 E. Gestione e manutenzione degli spazi ad uso ufficio per ospitare le PdL
D4: Componenti hw e sw della soluzione di DR	Disponibilità e manutenzione delle componenti hw e sw della soluzione di DR, in particolare: A1-A2 delle risorse elaborative hw, sw storage necessarie alla salvaguardia dei dati e delle applicazioni e alla ripartenza presso il sito di DR A3 delle postazioni di lavoro per personale tecnico coinvolto nel processo di ripartenza e gestione del Sistema Informativo, con caratteristiche analoghe a quelle del sito temporaneamente inagibile
D5 Servizi di replica dati per il DR	Il servizio di copia e trasferimento remoto a fini di backup e restore dei dati,immagine dei sistemi, applicazioni, può avvenire con modalità diverse: •trasferimento (elettronica e non) dei supporti di back up, relativa conservazione e possibilità di riconsegna •replica via rete del contenuto dei dischi
D6 Servizi di rete per il DR	Progettazione, realizzazione, gestione e manutenzione delle componenti di rete necessarie per la soluzione di DR.

LISTA SERVIZI	BREVE DESCRIZIONE E SOTTOSERVIZI
	Il servizio si articolerà nei seguenti sotto-servizi: A.Progettazione e dimensionamento della soluzione di rete; B.Fornitura, manutenzione e gestione, anche in modalità condivisa tra più amministrazioni, dei componenti di rete della soluzione di DR, inclusi quelli necessari alla gestione dell'instradamento alternativo degli accessi dalla periferia in caso di emergenza
D7 Servizi di gestione della soluzione di Dr sia in condizioni di normalità che in condizioni di emergenza	Il servizio deve assicurare la gestione ottimale della soluzione di DR al fine di assicurarne la piena efficienza. Il servizio potrà essere suddiviso in due sotto servizi: A. gestione della soluzione durante la normale operatività B. gestione dell'emergenza
D8 Servizi di verifica per le soluzioni di DR	Incarichi di verifica (audit) condotti da Terza Parte Indipendente sulle diverse componenti del DR/CO; Essi possono includere l'esecuzione di uno o più dei seguenti sotto-servizi: A.verifica dei piani di DR e CO -con simulazione del disastro -senza simulazione del disastro B.verifica delle infrastrutture di DR C.verifica dei test (di simulazione del disastro) D. verifica di conformità dei processi in atto presso l'organizzazione con quelli previsti dagli standard per il DR (ad es. ISO 22301) a fini di gap analysis o di certificazione

Tabella I – Quadro sinottico delle schede.

Le schede hanno un formato comune e sono articolate indicativamente come segue:

PARTE GENERALE	
DENOMINAZIONE	
DESCRIZIONE	
CORRISPONDENZA ITIL	
CORRISPONDENZA CPV	
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	
TIER	

PARTE TECNICA	
PRE-REQUISITI	
CARATTERISTICHE TECNICHE	
ADEMPIMENTI PREVISTI	
ADEMPIMENTI NON PREVISTI	
INDICATORI MINIMI DI SERVIZIO	
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	
COMPETENZE RICHIESTE	
TEMPI DI REALIZZAZIONE	

PARTE ECONOMICA (Componenti di costo)	
COSTI UNA TANTUM	
COSTI PERIODICI	
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	

Tabella II – Articolazione generale delle schede.

I servizi descritti dalle schede hanno una precisa collocazione nell'iter prefigurato dall' art. 50 bis del CAD.
In particolare, per le Amministrazioni che devono avviare il processo completo, a partire dalle attività per la predisposizione della richiesta di parere sullo studio di fattibilità tecnica della soluzione di DR, fino ai servizi di disponibilità del sito di DR e delle risorse elaborative con le relative attività di gestione, la collocazione

dei servizi rispetto alle varie fasi ppreviste dall'art. 50-bis del CAD puo' essere rappresentata come nella seguente Figura 1.

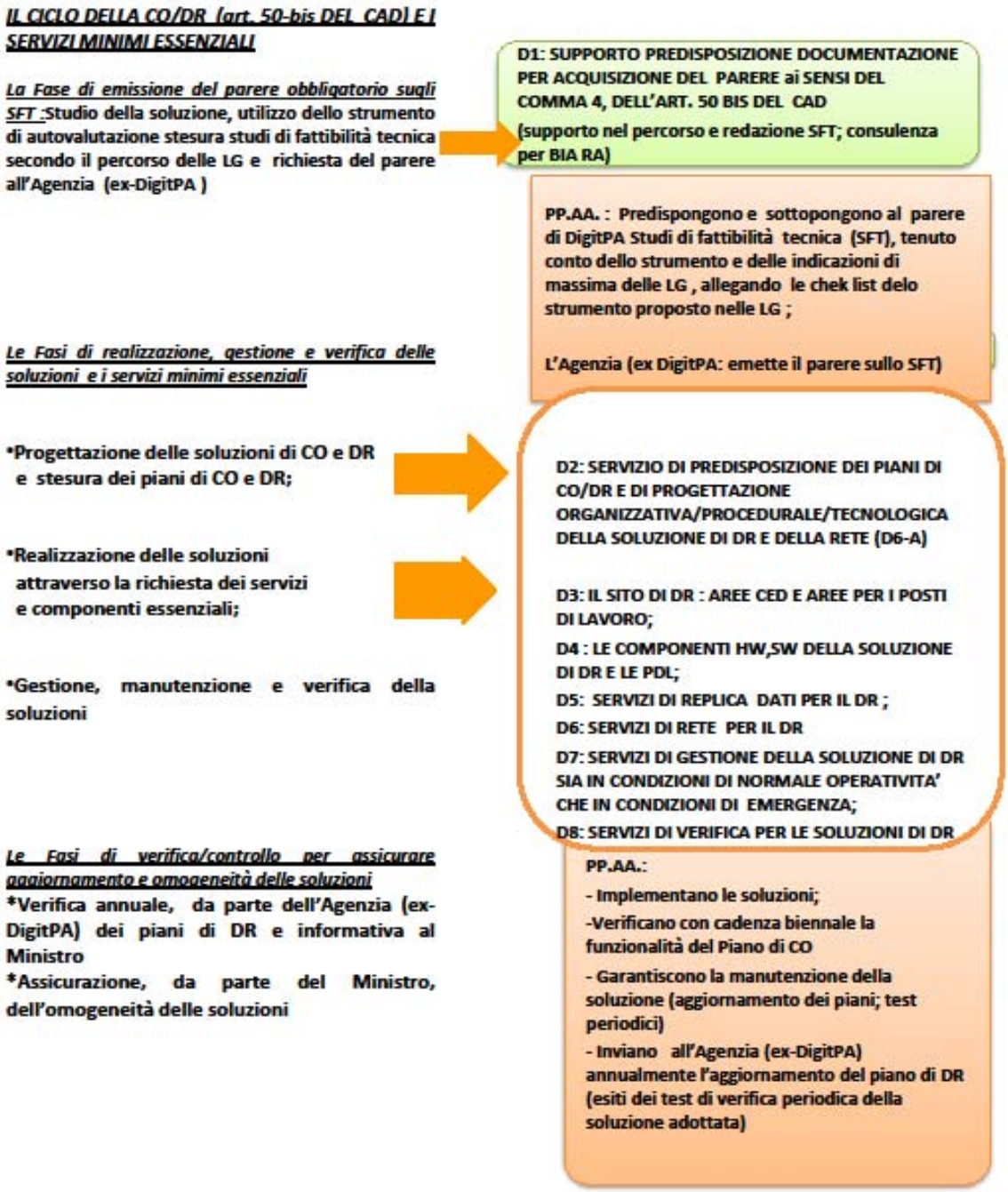


Figura 1 – Collocazione dei servizi descritti dalle schede all'interno dell'iter prefigurato dall' art. 50 bis del CAD.

Qualche esempio, senza la pretesa di essere esaustivi, consente di capire meglio i possibili utilizzi delle schede.
Si prenda il caso di un Amministrazione che debba partire ex novo nell'attuazione di quanto disposto dall'art. 50 bis ricorrendo a fornitori esterni: essa potrà attingere ai servizi di supporto e progettazione delle schede D1 e D2 e se al termine del percorso effettuato con il tool di autovalutazione (disponibile on-line presso il sito di DigitPA/Agenzia per l'Italia Digitale) e il supporto del fornitore, intenderà garantire la salvaguardia dei dati e delle applicazioni con soluzione del tier 3, dovrà dotarsi di un sito con le caratteristiche indicate nella scheda D3, delle componenti hardware e software e di rete, richiamate nelle schede D4 e D6 e replicare i dati secondo le modalita' descritte nella scheda D5. Laddove intendesse poi affidare in outsourcing la gestione della soluzione di DR, potrà attingere a servizi come quelli descritti nella scheda D7.

Si prenda altresì il caso di un Amministrazione che già disponga di un soluzione di DR del tipo tier 2, con un sito alternativo e un servizio di esecuzione e conservazione delle copie di backup dei propri dati e applicazioni. Se la stessa volesse verificare l'adeguatezza della soluzione di DR in essere, anche perché, ad esempio si è esteso il numero di procedimenti svolti esclusivamente in modalità informatica o perchè il quadro normativo ha ampliato il proprio asset di servizi e processi critici, la stessa potrà decidere di eseguire una nuova BIA o RA, attingendo ai sottoservizi della scheda D1, e eventualmente, una volta deciso di aggiornare la soluzione in essere, passando ad una soluzione tier 3, potrà attingere ai servizi e componenti della scheda D6, dotandosi dei servizi di rete per il DR ed eventualmente dei servizi di gestione della scheda D7 precedentemente citata.

Infine, ove Amministrazioni che già dispongono di soluzioni e servizi di DR volessero farsi coadiuvare nella proprie attività di controllo e monitoraggio dell'adeguatezza della soluzione, possono attingere a fornitori a ciò qualificati per i servizi di verifica delle soluzione di DR, come declinato nella scheda D8.

La Figura 2 seguente sintetizza l'impiego dei vari servizi.

Figura 2 – Il ciclo della CO/DR.

3. Il Tavolo Tecnico

Questo documento raccoglie le attivita' svolte dal Tavolo Tecnico istituito da DigitPA (ora Agenzia per l'Italia Digitale) per la definizione dei servizi minimi essenziali per l'adozione delle soluzioni di disaster recovery, in linea con l'art. 50-bis del CAD.

Il Tavolo Tecnico e' costituito da:

- Gruppo di Lavoro di DigitPA (ora Agenzia per l'Italia Digitale) composto dall'Ing. Alessandro Alessandroni, dalla D.ssa Cristina Di Domenico, dal Dott. Giovanni Rellini Lerz;

- ABI: Romano Stasi;
- ANCITEL: Caterina Guzzi;
- ANCI: Moira Benelli; G. Zaffi Borgetti
- ASSINTEL: Paolo Bussadori;
- CAPGEMINI: Enrico Giorgi;
- CONFINDUSTRIA DIGITALE: Giuseppe Neri (ASSINFORM); Francesco Giuffrè (ANITEC); in rappresentanza delle Aziende associate : Marco Schina (Almaviva); Marco Fabriani (CISCO); Roberto Loro (DEDAGROUP); Juan M.Cash (DELL); Antonio Sfameli (ERICSSON); Roberto Casini (ERICSSON); Aristeo Savelli (EXPRIVIA); Fabrizio Pasquini (FUJITSU); Giuseppe Di Natale (HP); Enrico Proietti De Marchis (HP); Maurizio Giovannetti (IBM) ; Francesco Scribano (IBM); Daniele Cortolezzis (INSIEL MERCATO); Enrico De Simoni (KPMG); Giuseppe Brunetti (NETAPP); Alberto Strani (SAMSUNG); Marina Settembre (SELEX ELSAG); Luigi Stilo (SIRTI), Federico Morena (TELECOM); Paola Colonna (TELECOM); Filippo Riccardo De Mango (FASTWEB);
- CISIS: Andrea Nicolini;
- COMUNE DI GROSSETO: Luca Ceccarelli; Ludwig Bargagli;
- COMUNE DI ROMA: Giancarlo Palombo, Daniele Liberini;
- CONSIP: Gaetano Santucci; Maria Stella Marotta; Domenico Pacchiarotti;
- CSI PIEMONTE: Vito Baglio;
- DELOITTE: Paola Galasso; Maurizio Biagini;
- GOOGLEMAIL: Emiliano Biocchetti; Maurizio Pio;
- INFORMATICA TRENTINA s.p.a.: Pierluigi Sartori;
- INTESA SAN PAOLO: Eugenio Livigni; Piero Giannoni;
- BANCA D' ITALIA: Nicola Di Sarli;
- REGIONE TOSCANA: Giovanni Armanino;
- SOGEI Massimo Greco, Gianpaolo Buccini;
- UPI: Luciano Archetti

Il Tavolo Tecnico e' stato coordinato dal Prof. ing. Antonio Orlandi di DigitPA (ora Agenzia per l'Italia Digitale).

4. Le Schede dei Servizi

Per ogni servizio minimo essenziale individuato in Tabella I segue la relativa scheda descrittiva.

SCHEDA SERVIZIO:D1

PARTE GENERALE

DENOMINAZIONE	D1 – Supporto alla predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4, dell'art. 50-bis del CAD.
DESCRIZIONE	Servizi di consulenza e supporto alla redazione della documentazione necessaria alla richiesta di parere di conformità. Il servizio si compone dei seguenti sotto-servizi: A.Supporto per: - la compilazione delle schede di autovalutazione; - la predisposizione dello Studio di Fattibilità Tecnica; - la predisposizione della Relazione Tecnica sullo stato di attuazione del CAD. B. Consulenza per Business Impact Analisys (BIA): Individuazione e valutazione servizi critici per la sopravvivenza del business; C. Consulenza per Risk Assessment (RA): Valutazione impatti di scenari che minacciano la sopravvivenza del business.
CORRISPONDENZA ITIL	Service Strategy Service Design IT Service Continuity Management
CORRISPONDENZA CPV	72150000-1 Servizi di consulenza per verifiche di sistemi informatici e servizi di consulenza per attrezzature informatiche; 72810000-1 Servizi di audit informatico; 72120000-2 Servizi di consulenza per il ripristino di attrezzature informatiche CPC 84990
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	SIF COP Continuità Operativa; CON Consulenza; PGE Gestione e processi organizzativi;
TIER CUI SI RIFERISCE IL SERVIZIO	1-6

PARTE TECNICA

<u>Sottoservizio A:</u> Supporto alla predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4, dell'art. 50-bis del CAD.

PRE-REQUISITI	• Individuazione e Classificazione preliminare dei Servizi • Mappa infrastruttura ICT • Elenco fornitori ICT • Possibili vincoli di carattere tecnico/economico espressi dall'Ente in fase di avvio del progetto • Documentazione organizzativa o di processo dell'Ente ove disponibile
CARATTERISTICHE TECNICHE	Il servizio ha l'obiettivo di fornire supporto all'Ente nella redazione della documentazione necessaria alla richiesta di parere di conformità sullo Studio di Fattibilità Tecnica così come previsto dall'art.50 bis comma 3 del CAD
ADEMPIMENTI PREVISTI	Il fornitore svolgerà i seguenti servizi: <u>Supporto all'Autovalutazione mediante</u>: a) Supporto alla corretta individuazione e classificazione dei Servizi dell'Ente: l'erogatore fornirà il supporto alla corretta individuazione e classificazione dei Servizi in base alla tipologia e complessità

	organizzativa e tecnologica dell'Ente; b) Interviste personale IT e referenti Servizi individuati Attraverso le interviste con i referenti individuati, l'erogatore raccoglierà le informazioni necessarie alla compilazione delle Schede. Durante le interviste l'erogatore svolgerà funzioni di mediatore e normalizzatore delle informazioni raccolte con riferimento alle criticità relative ed in riferimento alle Linee Guida DigitPA sulla Continuità Operativa; c) Compilazione Schede Servizi: con le informazioni raccolte, l'erogatore compilerà le schede di autovalutazione e le sottoporrà all'Ente per approvazione. <u>Supporto alla redazione dello Studio di Fattibilità Tecnica mediante:</u> a) Completamento mappa infrastrutturale ed architetturale dell'Ente. b) Definizione delle soluzioni tecniche ovvero selezione delle soluzioni di mercato idonee a realizzare le soluzioni tecnologiche individuate nella fase di valutazione dei servizi c) Macro-Analisi costi/benefici d) Redazione Studio di Fattibilità Tecnica secondo le Linee Guida DigitPA <u>Supporto alla redazione della Relazione Tecnica sullo stato di attuazione del CAD mediante</u>: a) raccolta delle informazioni necessarie attraverso interviste con il personale dell'Ente. b) Predisposizione della relazione in oggetto raccordando gli adempimenti previsti dal CAD con lo stato di effettiva attuazione o di quanto contenuto nello scenario programmatico dell'Ente.
ADEMPIMENTI NON PREVISTI	Il fornitore non svolgerà: a) Attività di analisi diretta sui sistemi informatici b) Attività di Business Impact Analisys o Risk Analisys c) Progettazione di dettaglio delle Soluzioni Tecniche individuate
INDICATORI MINIMI DEL SERVIZIO	• Completezza analisi rispetto agli adempimenti (in termini di: contenuti previsti dal template di STF e dal tool di autovalutazione, servizi in ambito) • Rispetto dei Tempi pianificati: scostamento rispetto alla pianificazione non superiore al 10% • Accuratezza nella compilazione dello strumento di autovalutazione • Redazione della documentazione STF che, nella descrizione della soluzione selezionata, riporti gli opportuni riferimenti a standard, criteri e linee guida nazionali ed internazionali comunemente riconosciuti in materia, • Indicazione del grado di attuazione di tutti gli adempimenti previsti dal CAD
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL) che consenta controlli intermedi sullo stato di avanzamento delle attività • Condivisione della documentazione predisposta , anche in versione "bozza". La documentazione fornita dovrà essere conforme ai template messi a disposizione da DigitPA. Il fornitore darà evidenza dei riferimenti di mercato adottati in merito alle soluzioni tecniche individuate.
COMPETENZE RICHIESTE	Competenze del fornitore: • IT audit • Progettuali tecnologiche in ambito ICT e di conoscenza del mercato; • Conoscenza del Nuovo Codice di Amministrazione Digitale Dlgs 235/2010 • Metodologiche sugli standard ISO e BS di riferimento; • Metodologiche sulle Linee Guida di DigitPA; • Organizzative e di processo in ambito PA; • Conoscenza processi e-Gov • Relazionali ;

	• Project Management; Disponibilità del personale dell'Ente Pubblico: • Referente settore IT • Referenti servizi individuati o classi di servizi
TEMPI DI REALIZZAZIONE	Indicativamente da 3 a 90 giorni (tempi elapsed), con le seguente stratificazione indicativa. Enti piccoli: 3-10 giorni Enti medi: 10-30 giorni Enti Grandi: 30-60 giorni Enti Grandissimi: 60 -90 giorni. Le tempistiche varieranno in funzione dei seguenti elementi: • Tipologia Ente • Complessità organizzativa Ente • Numero servizi individuati • Numero di interviste • Complessità tecnologica Ente

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Numero di giornate o a corpo con dimensionamento dell'effort in funzione di metriche individuate: • Tipologia Ente • Complessità organizzativa Ente • Numero di servizi e classi di servizi individuati • Complessità tecnologica Ente • Tipologia e complessità degli Scenari di Crisi individuati • Competenze delle risorse messe a disposizione dell'erogatore • Costi di trasferta
COSTI PERIODICI	Non previsti
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Non previsti, salvo quelli derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA
<u>Sotto servizi B e C:</u> Consulenza per BIA/RA

PRE-REQUISITI	• Individuazione e Classificazione preliminare dei Servizi • Mappa infrastruttura ICT • Elenco fornitori ICT • Possibili vincoli di carattere tecnico/economico espressi dall'Ente in fase di avvio del progetto • Documentazione organizzativa o di processo dell'Ente ove disponibile
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di supportare l'Ente nell'identificazione dei servizi critici, stimando i possibili impatti a fronte dell'interruzione del singolo servizio e definendo RTO, RPO e risorse di supporto per ciascun servizio analizzato.
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di supportare l'Ente nella definizione degli obiettivi di RTO e RPO dei servizi erogati (BIA) e una valutazione dei rischi che possono portare ad interruzioni di servizio o a violazioni della sicurezza (RA). I risultati di questa attività forniscono un supporto nella definizione delle strategie di ripristino. Per la BIA si prevedono le seguenti attività: • Identificare i siti di riferimento • Descrivere ogni servizio e stimarne l'impatto • Identificare le dipendenze tra i vari servizi • Stimare i tempi di ripristino del servizio

	• Definire RTO/RPO Per il RA le attività prevedono le seguenti attività: • Analisi delle minacce • valutazione della vulnerabilità • stima dell'impatto
ADEMPIMENTI NON PREVISTI	Definire la strategia di ripristino. I servizi di predisposizione dei piani e di progettazione organizzativa e tecnologica (servizio D2)
INDICATORI MINIMI DI SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL) • Completezza analisi rispetto al perimetro dei servizi e relativi asset, inclusi nell'analisi • Descrizione dei criteri in merito ad eventuali esclusioni di servizi dal perimetro considerato • Rispetto dei Tempi pianificati • Accuratezza nella redazione della documentazione prevista, inclusi i necessari riferimenti a standard e linee guida nazionali ed internazionali comunemente riconosciuti
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Governance e reporting dei lavori, rispetto del piano di attività • Livello di copertura e profondità della relazione finale • Possesso delle competenze professionali richieste (vedi sotto); • Verifica (audit) periodico (es. annuale) allo scopo di verificare che non siano intervenuti cambiamenti significati nei processi / obiettivi di business
COMPETENZE RICHIESTE (	• Competenze di IT audit • Competenze metodologiche sullo standard ITIL di riferimento • Competenze di organizzative e di processo in ambito PA
TEMPI DI REALIZZAZIONE	Le tempistiche sono variabili e dipendono dalla complessità della struttura organizzativa analizzata, come segue: Enti piccoli: 5 -20 giorni Enti medi: 10-40 giorni Enti Grandi: 30-60 giorni Enti Grandissimi: 60 - 180 giorni.

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Stimata sulla base delle giornate/uomo impiegate oppure a corpo, in funzione della complessità dell'organizzazione.
COSTI PERIODICI	Si suggerisce audit periodico (es. annuale) allo scopo di verificare che non siano intervenuti cambiamenti significati nei processi / obiettivi di business
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

SCHEDA SERVIZIO:D2	

PARTE GENERALE

DENOMINAZIONE	D2 -Servizio di Predisposizione dei piani di CO/DR e di progettazione organizzativa/procedurale/tecnologica della soluzione di DR"
DESCRIZIONE	Il servizio attiene alla produzione del piano di continuità operativa e di disaster recovery (CO/DR) partendo dallo studio di fattibilità (predisposto con i servizi della scheda D1) Per ottenere la produzione di tale piano sarà necessario prevedere la produzione di una piano di massima della soluzione tecnologica e del modello organizzativo per la gestione della crisi. Successivamente tali piani di massima dovranno essere dettagliati al fine di renderli operativi inserendo negli stessi tutte le informazioni necessarie a definire individualmente le singole attività/responsabilità. Dovrà infine essere descritto l'insieme delle procedure per la gestione del DR e il piano di CO nel suo insieme. Il servizio potrà articolarsi nei seguenti 6 Sotto-servizi: A. Progettazione di alto livello del modello organizzativo/procedurale B Progettazione di alto livello della soluzione tecnologica, con eventuale produzione di deliverable/studi per il consolidamento o la razionalizzazione del SI Primario (ove se ne evidenzi la necessità come passo propedeutico/prerequisito ai fini della realizzazione della soluzione di DR) C Progettazione di dettaglio del modello organizzativo/procedurale D Progettazione di dettaglio della soluzione tecnologica E Redazione delle procedure di DR F Redazione del piano di CO
CORRISPONDENZA ITIL	Ambito dei "Service Design" capitolo, "IT Service Continuity Management"
CORRISPONDENZA CPV	72120000-2 Servizi di consulenza per il ripristino di attrezzature informatiche
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP CON
TIER CUI SI RIFERISCE IL SERVIZIO	TIER 1, TIER 2, TIER 3, TIER 4, TIER 5, TIER 6 **Tier 1** prevede l'esecuzione, il trasporto e la conservazione dei backup (di dati, applicazioni e "immagine del sistema") in un sito diverso dal primario e, per i casi in cui si renda necessario assicurare il ripristino, la disponibilità di un sito "vuoto" attrezzato, pronto a ricevere le componenti e configurazioni necessarie, ove fosse richiesto, per far fronte all'emergenza (on demand). I backup (dei dati, delle applicazioni e dell'"immagine del sistema") sono conservati presso il sito remoto. In tale sito deve essere prevista la disponibilità, in caso di emergenza, sia dello storage su disco, dove riversare i dati conservati, sia di un sistema elaborativo in grado di permettere il ripristino delle funzionalità IT. **Tier 2**: la soluzione è simile a quella del Tier 1, vengono assicurate l'esecuzione, il trasporto, la conservazione dei backup (dei dati, delle applicazioni e dell'"immagine del sistema") e la disponibilità presso il sito dei sistemi e delle configurazioni da poter utilizzare per i casi in cui si renda necessario il ripristino, con la differenza che le risorse elaborative possono essere disponibili in tempi sensibilmente più brevi, viene garantito anche l'allineamento delle performance rispetto ai sistemi primari. **Tier 3**: la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai

	Tier precedenti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare). **Tier 4**: la soluzione prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. Le altre caratteristiche sono quelle del Tier 3, con la possibilità di aggiornamento dei dati (RPO) con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono). **Tier 5**: la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario (ferma restando la necessità di non prescindere dallo specifico contesto applicativo). **Tier 6**: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività in tempi molto ristretti.Le altre caratteristiche sono uguali a quelle del Tier 5.

PARTE TECNICA
Sotto-servizio A: Progettazione di alto livello del modello organizzativo/procedurale

PRE-REQUISITI	• Aver svolto le attività della scheda D1. • Aver ricevuto parere positivo da DigitPA in merito allo SFT inviato dall'Ente
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di supportare l'Ente nella progettazione strategica delle caratteristiche organizzative/procedurali della soluzione di DR e dei piani di CO/DR, coerentemente con i risultati dello studio di fattibilità e della BIA/RA di cui alla scheda D1, in considerazione della complessità e della criticità dell'Ente e delle risorse economiche disponibili. Obiettivo di tale sotto servizio è di produrre un documento organizzativo/procedurale di alto livello da portare all'approvazione dell'Ente, che tracci la soluzione organizzativa coerentemente con i requisiti dell'ente in materia di DR e CO.
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di supportare l'Ente al fine di: - identificare le caratteristiche organizzative/procedurali della soluzione di DR e dei piani di CO/DR, da adottare in relazione allo specifico contesto di riferimento - proporre una pianificazione di massima delle azioni necessarie per la messa in atto delle misure organizzative/procedurali utili alla realizzazione delle soluzioni di DR ed al piano di CO, da portare all'approvazione dell'Ente, come passo propedeutico alla progettazione di dettaglio. Gli aspetti da tenere in considerazione nell'analisi e nella progettazione suddetta dovranno essere i seguenti: • Tier prescelto nell'ambito dello SFT inviato a DigiPA; • applicazione delle linee strategiche e nei requisiti riportati nel documento di richiesta del parere a DigitPA • altri vincoli, requisiti ed opportunità impliciti o esplicitati dall'Ente (es. opportunità di soluzioni di mutuo soccorso, esclusione o inclusione di alcuni servizi dal perimento dei piani di CO/DR, ecc.), ove presenti; • definire se sono necessari uno o più siti CED alternativi presso cui attivare la soluzione di continuità, in considerazione degli aspetti logistici e di trasporto del

	personale e delle attrezzature necessari, qualora non già disponibili on-site; • analisi dei requisiti che influenzano il posizionamento del sito di DR (distanza minima, massima, servizi correlati, ecc) • individuazione delle funzioni essenziali, necessarie all'attivazione del sito CED alternativo; • contratti in essere; • ruoli e responsabilità del personale dell'Ente in relazione alle procedure previste dalla soluzione di DR e dal piano di CO, inclusi i ruoli di "vice"; • informazioni per la reperibilità del personale e dei fornitori; • definizione degli eventi di guasto, interruzione, disastro e dei relativi gradi di criticità e dell'attivazione delle relative procedure di DR/CO; • procedure di dichiarazione del disastro e compiti del Comitato di Crisi; • documentazione necessaria per la formalizzazione delle procedure e delle istruzioni; • necessità di eventuale formazione per utenti e per il personale IT e non IT; • strategia di test del piano di CO; • strategia di monitoraggio della predisposizione e manutenzione della soluzione di DR e dei piani di CO/DR; • procedure e soluzioni con scenari alternativi; • rischi accettati (non coperti) e scenari non previsti, esclusi dalla soluzione di CO/DR; • salute e sicurezza del personale e dei fornitori; • servizi di emergenza e di trasporto; • valutazione di eventuali polizze assicurative per l'Ente o per fornitori; • altri aspetti contrattuali connessi alla soluzione CO/DR; • aspetti organizzativi, procedurali e contrattuali connessi alle procedure di ripristino della normale operatività.
ADEMPIMENTI NON PREVISTI	Produzione delle specifiche di dettaglio della soluzione organizzativa/procedurale di DR e dei piani di CO/DR. Progettazione di massima di soluzioni organizzative/procedurali a copertura di rischi e di scenari esplicitamente non coperti e non compresi nel perimetro, coerentemente con le strategie, i vincoli ed i requisiti stabiliti dall'Ente.
INDICATORI MINIMI DI SERVIZIO	• Completezza del progetto rispetto agli adempimenti previsti e agli aspetti richiesti esplicitamente dall'Ente • Rispetto dei Tempi pianificati • Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Report descrittivo finale da portare all'approvazione dell'Ente • Report finale di rappresentazione della copertura dei requisiti Durante lo svolgimento del progetto: verifica dello stato di avanzamento del piano di lavoro e rispetto delle scadenze prestabilite. Alla consegna: verifica degli aspetti presi in considerazione dalla progettazione, rispetto alle aree di analisi dichiarate dagli "adempimenti previsti" del sotto-servizio.
COMPETENZE RICHIESTE	• Competenze metodologiche sullo standard ITIL di riferimento • Competenze organizzative e di processo in ambito PA • Competenze di project management • Competenze sulle soluzioni organizzative di DR e CO • Competenze di legali e contrattuali • Competenze di logistica • Competenze di salute e sicurezza sul lavoro
TEMPI DI REALIZZAZIONE	Un tempo *elapsed* variabile tra: Piccolo Ente: da 2 mesi a 3 mesi Grande Ente: da 3 mesi a 6 mesi Medio Ente: da 4 mesi a 8 mesi Ente Grandissimo: da 6 mesi a 12 mesi

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	A corpo o gg/u (usualmente a corpo).
COSTI PERIODICI	Nessuno
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni. Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA
Sotto-servizio B: Progettazione di alto livello della soluzione tecnologica

PRE-REQUISITI	Aver svolto le attività della scheda D1. Aver ricevuto parere positivo da DigitPA sullo SFT inviato dall'Ente Svolgere le attività del sottoservizio A (High Level) della scheda D6 (preferibilmente in parallelo)
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di supportare l'Ente nella progettazione strategica delle caratteristiche tecnologiche della soluzione di DR e dei piani di CO/DR, coerentemente con i risultati dello studio di fattibilità e della BIA/RA di cui alla scheda D1, in considerazione della complessità e della criticità dell'Ente e delle risorse economiche disponibili. Obiettivo di tale sotto servizio è di produrre un documento tecnico di alto livello da portare all'approvazione dell'Ente, che tracci la soluzione organizzativa/procedurale coerentemente con i requisiti dell'ente in materia di DR e CO.
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di supportare l'Ente al fine di: - identificare le caratteristiche tecnologiche della soluzione di DR e dei piani di CO/DR, da adottare in relazione allo specifico contesto di riferimento; -evidenziare l'eventuale necessità di eseguire interventi di consolidamento/adeguamento sul sito principale al fine di ridurre i costi e/o aumentare l'affidabilità e le prestazioni del DR; - proporre una pianificazione di massima delle azioni necessarie per la messa in atto delle misure tecnologiche utili alla realizzazione delle soluzioni di DR ed ai piani di CO/DR, da portare all'approvazione dell'Ente, come passo propedeutico alla progettazione di dettaglio. Gli aspetti da tenere in considerazione nell'analisi e nella progettazione suddetta, oltre ai pre-requisiti tecnici dovranno essere i seguenti: • altri vincoli, requisiti ed opportunità di carattere tecnico impliciti o esplicitati dall'Ente (es. efficienze energetica, opportunità di soluzioni di mutuo soccorso, esclusione o inclusione di alcuni servizi dal perimento dei piani di CO/DR, ecc.), ove presenti; • presenza di uno o più siti CED alternativi presso cui attivare la soluzione di continuità; • analisi dei requisiti che influenzano il posizionamento del sito di DR (distanza minima, massima, servizi correlati ecc) • competenze specialistiche ICT, necessarie all'attivazione del sito CED alternativo; • complessità delle soluzioni tecniche in uso; • eventuale presenza di uno o più outsourcer ICT; • contratti in essere, strategia di backup di dati e programmi; • misure di sicurezza logica e di integrità dei dati da ripristinare; • livelli minimi di servizio elaborativi, di connettività e di disponibilità dei

	dati; • strategia di test e di monitoraggio del corretto funzionamento dei dispositivi hardware, software e di connettività (dati e voce) previsti dalle soluzioni tecnologiche che si vogliono adottare; • identificazione delle componenti tecnologiche e di rete (vedi servizio di progettazione rete); • aspetti tecnologici connessi alle modalità di ripristino della normalità; • strategia di test della soluzione di DR.
ADEMPIMENTI NON PREVISTI	Produzione delle specifiche tecniche di dettaglio per la realizzazione della soluzione tecnologica di DR e dei piani di CO/DR Progettazione di massima di soluzioni tecnologiche di DR e dei piani di CO/DR a copertura di dati e sistemi non compresi nel perimetro, coerentemente con le strategie, i vincoli ed i requisiti stabiliti dall'Ente.
INDICATORI MINIMI DI SERVIZIO	• Completezza del progetto rispetto agli adempimenti previsti e agli aspetti richiesti esplicitamente dall'Ente • Rispetto dei Tempi pianificati • Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Report descrittivo finale da portare all'approvazione dell'Ente • Report finale di rappresentazione della copertura dei requisiti Durante lo svolgimento del progetto: verifica dello stato di avanzamento del piano di lavoro e rispetto delle scadenze prestabilite. Alla consegna: verifica degli aspetti presi in considerazione dalla progettazione, rispetto alle aree di analisi dichiarate dagli "adempimenti previsti" del sotto-servizio
COMPETENZE RICHIESTE	• Competenze metodologiche sullo standard ITIL di riferimento • Competenze tecnologiche in ambito PA • Competenze di project management • Competenze sulle soluzioni tecniche di DR e CO • Competenze di sistemistiche e di telecomunicazione • Competenze di applicative e di database • Competenze contrattuali in ambito ICT
TEMPI DI REALIZZAZIONE	Un tempo *elapsed* variabile tra: Piccolo Ente: da 2 mesi a 3 mesi Medio Ente: da 3 mesi a 6 mesi Grande Ente: da 4 mesi a 8 mesi Ente Grandissimo: da 6 mesi a 12 mesi.

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	A corpo o gg/u..
COSTI PERIODICI	Nessuno
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni. Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA
Sottoservizio C: Progettazione di dettaglio del modello organizzativo/procedurale

PRE-REQUISITI	Aver svolto le attività del sotto servizio A della presente scheda D2: Progettazione di alto livello della soluzione organizzativa/procedurale
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di supportare l'Ente nel definire il progetto

	organizzativo/procedurale di dettaglio della soluzione di DR/CO. Il progetto deve approfondire le tematiche introdotte nel progetto organizzativo/procedurale di massima definendo nel massimo dettaglio i ruoli, le singole responsabilità, le modalità di intervento e quanto altro necessario a rendere operativo il modello organizzativo/procedurale.
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di supportare l'Ente affinché sia possibile produrre le specifiche di dettaglio della soluzione organizzativa/procedurale di DR/CO e calarle nel contesto dell'Ente. In particolare, dovranno essere pianificate e definite nel dettaglio le seguenti attività: • assegnazione di ruoli e responsabilità di dettaglio, secondo i diversi scenari coperti • accordi contrattuali necessari con fornitori esterni • accordi contrattuali sindacali necessari per la gestione del personale • del dettaglio del piano di formazione • attuazione delle misure di salute e sicurezza delle risorse umane • servizi di emergenza e trasporto da attivare in caso di disastro • disponibilità delle risorse umane interne ed esterne • redazione della documentazione in merito a politiche, linee guida, procedure ed istruzioni di dettaglio da attuare in caso di disastro • disponibilità della documentazione suddetta e dei contatti del personale chiave e dei fornitori • test e monitoraggio dei piani di CO/DR
ADEMPIMENTI NON PREVISTI	Requisiti relativi ad aspetti non inclusi nella progettazione di livello dettaglio
INDICATORI MINIMI DI SERVIZIO	• Completezza del progetto rispetto agli adempimenti previsti e agli aspetti richiesti esplicitamente dall'Ente • Rispetto dei Tempi pianificati • Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Report descrittivo finale da portare all'approvazione dell'Ente • Documentazione di dettaglio per i singoli aspetti/cantieri progettati Durante lo svolgimento del progetto: verifica dello stato di avanzamento del piano di lavoro e rispetto delle scadenze prestabilite. Alla consegna: verifica dell'approfondimento degli aspetti presi in considerazione dalla progettazione di alto livello,
COMPETENZE RICHIESTE	• Competenze metodologiche sullo standard ITIL di riferimento • Competenze organizzative e di processo in ambito PA • Competenze di project management • Competenze sulle soluzioni organizzative di DR e CO • Competenze di legali e contrattuali • Competenze di logistica Competenze di salute e sicurezza sul lavoro
TEMPI DI REALIZZAZIONE	Un tempo *elapsed* variabile tra: Piccolo Ente: da 1 mesi a 2 mesi Medio Ente: da 2 mesi a 4 mesi Grande Ente: da 3 mesi a 6 mesi Ente Grandissimo: da 4 mesi a 8 mesi.

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	A corpo o gg/u
COSTI PERIODICI	Nessuno
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni.

	Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

---

PARTE TECNICA
Sottoservizio D: Progettazione di dettaglio della soluzione tecnologica

PRE-REQUISITI	Aver svolto le attività del sotto servizio B della presente scheda D2: Progettazione di alto livello della soluzione tecnologica Svolgere le attività del sottoservizio A della scheda D6 (preferibilmente in parallelo)
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di supportare l'Ente nel definire il progetto tecnologico di dettaglio della soluzione di CO/DR. Il progetto deve approfondire le tematiche introdotte nel progetto tecnologico di massima definendo nel massimo dettaglio le tecnologie più idonee e quanto altro necessario a rendere operativo il modello tecnologico.
ADEMPIMENTI PREVISTI	I Il fornitore avrà il compito di supportare l'Ente affinché sia possibile produrre le specifiche di dettaglio della soluzione tecnologiche di DR/CO e calarle nel contesto dell'Ente. Il progetto nel fornire indicazioni sulla tipologia di sito di DR di cui si deve dotare l'Ente deve, oltre tenere in considerazione le indicazioni derivanti dall'adozione di normative e standard tipo TIA942 e ISO24762, definire almeno gli aspetti riportati in allegato A alla presente scheda D2. Altro aspetto rilevante nella fase di progettazione è la riduzione dei consumi e la definizione di una soluzione il più possibile eco-compatibile Il progetto deve prevedere la produzione di deliverable/studi per il consolidamento o la razionalizzazione del SI Primario (ove se ne evidenzi la necessità come passo propedeutico/prerequisito ai fini della realizzazione della soluzione di DR) Il consolidamento può riguardare sia gli aspetti infrastrutturali del sito primario che la configurazione hardware/software della soluzione informatica In particolare, dovranno essere pianificate e definite nel dettaglio le seguenti attività: • requisiti di dettaglio delle architetture tecnologiche di DR da adottare; • requisiti di dettaglio delle misure di sicurezza logica, fisica ed ambientale da attuare a protezione dei dispositivi ICT; • requisiti tecnici di dettaglio delle procedure di backup e restore di dati e programmi; • le specifiche degli accordi da prendere con i fornitori con riferimenti alla parte tecnologica dei contratti; • requisiti di dettaglio sui livelli minimi di servizio; • requisiti tecnici di dettaglio sulla procedura di ripristino della normalità; • attuazione delle procedure di back-up e ripristino il progetto deve tenere conto, soprattutto per i Tier 5 e 6, della progettazione di rete per la definizione della distanza massima tra i siti.
ADEMPIMENTI NON PREVISTI	Requisiti relativi ad aspetti non inclusi nella progettazione di dettaglio
INDICATORI MINIMI DI SERVIZIO	• Completezza del progetto rispetto agli adempimenti previsti e agli aspetti richiesti esplicitamente dall'Ente • Rispetto dei Tempi pianificati

	• Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Report descrittivo finale da portare all'approvazione dell'Ente • Documentazione di dettaglio per i singoli aspetti/cantieri progettati Durante lo svolgimento del progetto: verifica dello stato di avanzamento del piano di lavoro e rispetto delle scadenze prestabilite. Alla consegna: verifica dell'approfondimento degli aspetti presi in considerazione dalla progettazione di alto livello,
COMPETENZE RICHIESTE	• Competenze metodologiche sullo standard ITIL di riferimento • Competenze tecnologiche in ambito PA • Competenze di project management • Competenze sulle soluzioni tecniche di DR e CO • Competenze di sistemistiche e di telecomunicazione • Competenze di applicative e di database • Competenze contrattuali in ambito ICT
TEMPI DI REALIZZAZIONE	Un tempo *elapsed* variabile tra: Piccolo Ente: da 1 mesi a 2 mesi Medio Ente: da 2 mesi a 4 mesi Grande Ente: da 4 mesi a 8 mesi Ente Grandissimo: da 6 mesi a 12 mesi

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	A corpo o gg/u
COSTI PERIODICI	nessuno
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni. Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA
Sottoservizio E: Redazione delle procedure di DR

PRE-REQUISITI	Aver svolto le attività dei sotto- servizi C e D della scheda presente D2: Progettazione di dettaglio della soluzione tecnica ed organizzativa/procedurale di DR/CO
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di supportare l'Ente nella redazione delle procedure di DR, coerentemente con i risultati della progettazione tecnica ed organizzativa di dettaglio
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di redigere un documento organico in cui siano descritte tutte le procedure di DR, referenziando opportunamente i requisiti tecnici ed organizzativi/procedurali precedentemente definiti e gli strumenti tecnici ed organizzativi predisposti dall'Ente in attuazione a requisiti suddetti. Il fornitore dovrà erogare sessioni di formazione tecnica dell'ambiente di DR in conformità a quanto individuato dalle fasi di progettazione precedenti
ADEMPIMENTI NON PREVISTI	Il fornitore non redigerà procedure al di fuori dal perimetro delle soluzioni di DR definite ed approvate nell'ambito della strategia di DR (di cui ai sotto-servizi A e B) e dei requisiti tecnici ed organizzativi/procedurali di dettaglio (di cui ai sotto servizi C e D).
INDICATORI MINIMI DI SERVIZIO	• Completezza del documento finale rispetto agli aspetti strategici ed ai requisiti definiti nell'ambito dei sotto-servizi precedenti, in materia di DR • Rispetto dei Tempi pianificati

	• Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Documento strutturato "Procedure di DR" dell'Ente • Allegati tecnici del documento
COMPETENZE RICHIESTE	• Competenze metodologiche sullo standard ITIL di riferimento • Competenze tecnologiche in ambito PA • Competenze sulle soluzioni tecniche di DR e CO • Competenze sistemistiche e di telecomunicazione • Competenzeapplicative e di database
TEMPI DI REALIZZAZIONE	Un tempo *elapsed* variabile tra: Piccolo Ente: da 1 mesi a 2 mesi Medio Ente: da 2 mesi a 4 mesi Grande Ente: da 4 mesi a 8 mesi Ente Grandissimo: da 6 mesi a 12 mesi

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	A corpo o gg/u
COSTI PERIODICI	Canone, da definire in caso sia inclusa anche la manutenzione
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni. Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA
Sottoservizio F: Redazione del piano di CO

PRE-REQUISITI	Aver svolto le attività dei sotto- servizi C e D della scheda presente D2: Progettazione di dettaglio della soluzione tecnica ed organizzativa di DR/CO
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di supportare l'Ente nella redazione del piano di continuità operativa, coerentemente con i risultati della progettazione tecnica ed organizzativa di dettaglio
ADEMPIMENTI PREVISTI	Il fornitore dovrà redigere il piano di continuità operativa con le seguenti caratteristiche: - siano affrontati tutti gli aspetti, informatici ed organizzativi/procedurali - siano definite le modalità di erogazione dei servizi in caso di disastro - siano referenziati i requisiti tecnici ed organizzativi/procedurali precedentemente definiti - siano referenziati gli strumenti tecnici ed organizzativi/procedurali predisposti dall'Ente in attuazione a requisiti suddetti - il piano di CO deve contenere le procedure di DR
ADEMPIMENTI NON PREVISTI	Il fornitore non redigerà parti del piano di CO che siano al di fuori dal perimetro così come definito ed approvato nell'ambito della strategia di CO (di cui ai sotto-servizi 1 e 2) e dei requisiti tecnici ed organizzativi/procedurali di dettaglio (di cui ai sotto servizi 3 e 4).
INDICATORI MINIMI DI SERVIZIO	• Completezza del documento finale rispetto agli aspetti strategici ed ai requisiti definiti nell'ambito dei sotto-servizi precedenti, in materia di CO • Rispetto dei Tempi pianificati • Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Documento strutturato "Piano di CO" dell'Ente • Allegati tecnici del documento Il documento suddetto e/o i suoi allegati tecnici deve comprendere i

	contenuti di cui al documento "Procedure di DR".
COMPETENZE RICHIESTE	• Competenze metodologiche sullo standard ITIL di riferimento • Competenze organizzative e di processo in ambito PA • Competenze di project management • Competenze sulle soluzioni organizzative di DR e CO • Competenze di legali e contrattuali • Competenze di logistica • Competenze di salute e sicurezza sul lavoro
TEMPI DI REALIZZAZIONE	Un tempo *elapsed* variabile tra: Piccolo Ente: da 1 mesi a 2 mesi Medio Ente: da 2 mesi a 4 mesi Grande Ente: da 4 mesi a 8 mesi Ente Grandissimo: da 6 mesi a 12 mesi

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	A corpo o gg/u
COSTI PERIODICI	Canone, da definire in caso sia inclusa anche la manutenzione
COSTI PER EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni. Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

Allegato A scheda D2

1	Definizione della distanza minima dal sito primario
2	Numero di siti da utilizzare (uno o più)
3	Definizione delle caratteristiche tecniche e di continuità dell'impianto luci emergenza
4	Definizione del minimo di lux che l'impianto di illuminazione deve fornire
5	Caratteristiche tecniche della pavimentazione flottante, con precisa indicazione delle dimensioni dei moduli, della portata e del valore di punta relativamente al carico, dell'altezza utile.
6	Indicazione del valore minimo di carico che il solaio deve supportare
7	Caratteristiche del Sistema di rilevazione antiallagamento
8	Necessità o meno di punti manuali di attivazione allarmi e relative caratteristiche
9	Presenza di segnalatori acustici per gestione emergenze con indicazione delle caratteristiche
10	Caratteristiche del tetto in termini di impermeabilizzazione
11	Adeguato impianto antifulmini
12	Eventuale necessità di locali per personale dell'amministrazione
13	Caratteristiche dell'infrastruttura elettrica
14	Autonomia minima in caso di indisponibilità di rifornimenti di acqua, gas, carburante, elettricità, ecc.
15	Numero di sorgenti alimentazione server e/o rack e loro caratteristiche
16	Caratteristiche del sistema di condizionamento (switch, potenza elettrica minimale, sensori temperatura, ecc.)
17	Sistema di monitoraggio continuo e relativi allarmi per la temperatura nell'intero datacenter.
18	Caratteristiche del sistema di rilevazione antincendio (rilevatori fumi, calore, ecc)
19	Caratteristiche del sistema di spegnimento incendi
20	Caratteristiche del sistema di monitoraggio impianti.
21	Caratteristiche del sistemi di videosorveglianza interna ed esterna.
22	Definizione formalizzata delle aree del datacenter (aree CED a massima sicurezza, area carico/scarico, ecc)
23	Requisiti minimi per il controllo accessi alla struttura e specificatamente al CED.

SCHEDA SERVIZIO: D3

PARTE GENERALE

DENOMINAZIONE	D3 - Sito di Disaster Recovery: aree CED e aree attrezzate per i posti di lavoro
DESCRIZIONE	Disponibilità e mantenimento di aree CED e aree per PdL, nel quale siano installati o installabili i sistemi necessari a ripristinare i servizi informatici identificati nello Studio di Fattibilità e dettagliati nel progetto esecutivo. Il servizio potrà articolarsi nei seguenti Sotto-servizi: A. Disponibilità della struttura edile e impiantistica per gli spazi del sito di DR B. Esecuzione degli eventuali interventi sul sito primario e sul sito di DR comprensiva, ove necessario, della predisposizione dell'infrastruttura tecnico-logistica, per renderlo conforme ai requisiti minimi obbligatori riportati in allegato alla presente scheda D3, definiti – a seguito dei servizi di progettazione della scheda D2 – come passo propedeutico/prerequisito della realizzazione della soluzione di DR C. Gestione e manutenzione del sito di DR D. Disponibilità di spazi ad uso ufficio destinati ad ospitare le PdL secondo le modalità descritte nella scheda D4 E. Gestione e manutenzione degli spazi ad uso ufficio per ospitare le PdL
CORRISPONDENZA ITIL	Service Design – IT Service Continuity Management Service Operation
CORRISPONDENZA CPV	72510000-3 72570000-1 71315210-4 71700000-5
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP CON PAQ
TIER CUI SI RIFERISCE IL SERVIZIO	TIER 1, TIER 2, TIER 3, TIER 4, TIER 5, TIER 6 • Tier 1 e 2: non ci sono collegamenti di rete fra siti (primario e di DR). Il tempo per avere la disponibilità del sito in caso di disastro influisce sul valore di RTO. • Tier 3, 4, 5 e 6:prevedono collegamenti di rete fra i siti (primario e di DR). Per i tier 5 e 6 allo stato attuale della tecnologia non si può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che per i tier 5 e 6 la modalità di allineamento (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario (ferma restando la necessità di non prescindere dallo specifico contesto applicativo).

PARTE TECNICA
Sotto-servizio A: Disponibilità della struttura edile e impiantistica per gli spazi del sito di DR

PRE-REQUISITI	Verifica della rispondenza della struttura edile e impiantistica del sito alle caratteristiche tecniche richieste dall'Amministrazione nel progetto esecutivo
CARATTERISTICHE TECNICHE	Fornitura di spazi CED, che possono essere: • **dedicati**: fornitura di specifici spazi concordati con l'Amministrazione che soddisfino i requisiti progettuali. L'area sarà dedicata in maniera univoca all'Amministrazione • **condivisi**: fornitura di spazi che rispondano alle specifiche progettuali, ma che possono ospitare apparati e sistemi condivisibili anche con altri Enti Le macro aree che devono essere considerate per determinare l'idoneità del sito

	sono: <u>SICUREZZA FISICA</u> - distanza dal DC primario tale da soddisfare la protezione dagli scenari di disastro identificati in fase di Studio di Fattibilità - dotazione di misure tecnologiche e procedurali di sicurezza fisica idonee a proteggerlo da intrusioni dall'esterno (sicurezza perimetrale) o da accessi di persone non autorizzate alle aree riservate (locali CED, vani tecnici) - dispositivi di prevenzione, rilevamento e segnalazione contro il pericolo di incendio ed allagamento dei locali <u>SERVIZI LOGISTICI</u> - presidio e controllo accessi h24 - servizi di telefonia anche IP - gestione ricevimento e stoccaggio apparati - raggiungibilità e mezzi di trasporto - aree interne di ristoro - strutture ricettive alberghiere e ristorazione in zona <u>AFFIDABILITÀ INFRASTRUTTURE TECNOLOGICHE</u> - ridondanza sistemi di continuità elettrica - ridondanza sistemi di condizionamento Le caratteristiche ed i requisiti generali sono riportati nella scheda D2 e servono da riferimento durante la progettazione esecutiva. I requisiti minimi obbligatori in caso di Data Center di un Fornitore sono riportati in allegato alla presente scheda D3
ADEMPIMENTI PREVISTI	• Possesso dei titoli autorizzativi previsti dalle leggi e regolamenti vigenti all'atto della verifica di idoneità del sito • Certificazione periodica degli impianti tecnologici (elettrico, condizionamento, rilevazione fumi, antincendio, sicurezza) • Verifica costante dell'adeguatezza del sito in termini di potenza elettrica e refrigerante erogata • Attuazione del processo di gestione degli accessi del personale e anti-intrusione del sito
ADEMPIMENTI NON PREVISTI	• Connettività WAN-SPC • Modifiche agli impianti tecnologici non conseguenti alla normale attività di manutenzione ordinaria o di riparazione • Eventuale esecuzione degli interventi individuati come propedeutici sul sito principale per renderlo conforme ai requisiti definiti nei servizi della scheda D2 come passo propedeutico/prerequisito della realizzazione della soluzione di DR
INDICATORI MINIMI DI SERVIZIO	• Tempi di messa a disposizione del sito per alloggiare gli apparati ed i sistemi di DR a partire dal momento della richiesta dell'Ente secondo i valori di RTO e RPO richiesti dall'Ente. • Percentuale di disponibilità e funzionamento del sito nella finestra temporale di servizio richiesta dall'Amministrazione/Ente
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Documentazione attestanti la conformità ai requisiti e titoli autorizzativi • Sopralluoghi per la verifica delle caratteristiche di ridondanza e autonomia dei sistemi di continuità elettrica e condizionamento. • Verifica del rispetto delle misure di sicurezza fisica e dei servizi logistici richiesti.
COMPETENZE RICHIESTE	• Competenze sulle norme per l'attrezzaggio e gestione di spazi CED • Competenze impianti tecnologici • Competenze sulle soluzioni tecnologiche di disaster recovery
TEMPI DI REALIZZAZIONE	Un tempo elapsed variabile da 1 a 6 mesi in funzione delle opere da realizzare, per soddisfare la quantità di spazio richiesto, presso un sito già esistente.

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	• Costi di investimento per opere di adeguamento locali e servizi logistici richiesti dall'Amministrazione • Eventuali costi non standard dovuti alla fase di startup della soluzione
COSTI PERIODICI	• Costi a canone per l'uso dei locali CED (affitto dei locali, consumi, sorveglianza, oneri contrattuali)
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVI	• Costi di investimento per opere di adeguamento locali, servizi logistici a seguito di variazioni delle esigenze dell'Amministrazione, quali ad esempio: incremento degli spazi richiesti, variazioni dei SLA • Adeguamento dei canoni per l'uso dei locali del Data Center dovuto ad incrementi dei costi per i consumi operato dal Fornitore delle utility pubbliche

PARTE TECNICA

Sotto-servizio B: Esecuzione degli interventi sul sito primario o sul sito di DR

PRE-REQUISITI	Verifica delle caratteristiche della struttura edile e impiantistica del sito / dei siti o e analisi degli interventi dettagliati nel progetto esecutivo (Gap Analysis)
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di realizzare gli interventi sul sito primario per renderlo conforme ai requisiti definiti, nei servizi della scheda D2, come passo propedeutico/prerequisito della realizzazione della soluzione di DR
ADEMPIMENTI PREVISTI	il fornitore dovrà eseguire gli interventi individuati in linea con le caratteristiche richieste per adeguare il sito/i siti ai requisiti espressi nella progettazione di massima e esecutiva come descritto nella scheda D2 e come riportato in allegato alla presente scheda
ADEMPIMENTI NON PREVISTI	Le componenti hw,sw di rete di cui alle schede D4 e D6
INDICATORI MINIMI DI SERVIZIO	• Report sullo Stato Avanzamento Lavori (SAL) • Collaudo degli interventi e delle opere realizzate
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Verifica della conformità degli interventi con la progettazione esecutiva e con il piano di collaudo delle opere
COMPETENZE RICHIESTE	• Competenze sulle norme per l'attrezzaggio e gestione di spazi CED • Competenze sulla realizzazione di impianti tecnologici • Competenze sulle soluzioni tecnologiche di disaster recovery
TEMPI DI REALIZZAZIONE	Dipendente dal tipo e consistenza degli interventi di adeguamento richiesti

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	• A corpo o gg/u attività di gestione del cantiere • Costi di investimento per l'esecuzione degli interventi richiesti per predisporre l'infrastruttura e rendere il sito conforme ai requisiti definiti
COSTI PERIODICI	Nessuno
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali, da definire in base alle esigenze dell'Ente

Allegato alla scheda D3
Requisiti minimi obbligatori in caso di Data Center di un Fornitore

1	Garanzia di conformità a tutti i permessi necessari (agibilità, VVFF, ecc.)
2	Garanzia di antisismicità coerente col livello sismico del luogo, garanzia di località non soggetta a tempeste di ghiaccio e neve, allagamenti, alluvioni, frane
3	Presenza impianto luci emergenza
4	Esistenza della pavimentazione flottante
5	Sistema di rilevazione antiallagamento
6	Presenza di punti manuali di attivazione allarmi
7	Presenza di segnalatori acustici per gestione emergenze
8	Infrastruttura elettrica ridondata e protetta con UPS (o altri sistemi di continuità) e gruppo elettrogeno per tutti

	gli impianti
9	Doppia sorgente alimentazione per server e/o rack
10	alloggiamenti TLC dedicati
11	sistema di condizionamento centralizzato con diffusori nelle sale CED.
12	Sistema di monitoraggio continuo e relativi allarmi per la temperatura nell'intero datacenter.
13	Protezione esterna con sistema antiscavalcamento e illuminazione.
14	Sistemi di videosorveglianza h24
15	Definizione formalizzata delle aree del datacenter (accesso primario, accesso forniture, uffici e sale riunioni, sale impianti e controlli, sale macchine con relativi sistemi di controllo accessi anche biometrico e sbarramento).
16	Identificazione di uno o più responsabile/i delle aree del sito per le autorizzazioni necessarie all'accesso. Procedura di accesso alle aree per limitare l'accesso alle persone autorizzate dal responsabile, con almeno le seguenti classi di accesso: • personale del prestatore, • personale clienti del prestatore, • personale delegato dal prestatore (ad esempio personale che esegue manutenzione/riparazione, ecc.); • visitatori. La procedura deve anche regolare la gestione di badge/passi temporanei e le modalità di accompagnamento di personale esterno (clienti, manutenzione, ecc.) alle varie aree del sito da parte di personale del prestatore. La/le procedura/e deve/devono essere inserite nella politica di sicurezza dell'impresa, di cui è necessario dare evidenza.
17	Conformità alla legge 81/2008, addestramento del personale e attrezzaggio per il pronto soccorso come previsto dalla legge 388/2003, locale di pronto soccorso
18	Presenza reception e/o sorveglianza armata h24

SCHEDA SERVIZIO: D4

PARTE GENERALE

DENOMINAZIONE	D4: Componenti HW e SW della soluzione di DR
SOTTO SERVIZI	• A1) Disponibilità risorse hw e sw • A2) Gestione e manutenzione risorse hw e sw • A3) Disponibilità e manutenzione dei soli posti di lavoro presso il sito di DR nelle fasi di test e in emergenza
DESCRIZIONE	• A1-A2 risorse elaborative hw, sw storage necessarie alla salvaguardia dei dati e delle applicazioni e alla ripartenza presso il sito di DR • A3 disponibilità postazioni di lavoro per personale tecnico coinvolto nel processo di ripartenza e gestione del Sistema Informativo del Cliente, con caratteristiche analoghe a quelle del sito temporaneamente inagibile
CORRISPONDENZA ITIL	Service Design – IT Service Continuity Management Service Operation
CORRISPONDENZA CPV	72150000-1 72514000-1
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP CON PAQ
TIER	Tier 1: è la soluzione minimale coerente con quanto previsto dall'articolo 50-bis. Prevede il backup dei dati presso un altro sito tramite trasporto di supporto (nastro o altro dispositivo). I dati sono conservati presso il sito remoto. In tale sito deve essere prevista la disponibilità, in caso di emergenza, sia dello storage su disco, dove riversare i dati conservati, sia di un sistema elaborativo in grado di permettere il ripristino delle funzionalità IT. Vengono quindi assicurate l'esecuzione e conservazione dei backup e, per i casi in cui si renda necessario assicurare il ripristino, la disponibilità di un sito "vuoto" attrezzato, pronto a ricevere le componenti e configurazioni necessarie, ove fosse richiesto, per far fronte all'emergenza (on demand). Tier 2: la soluzione è simile a quella del Tier 1, con la differenza che le risorse elaborative possono essere disponibili in tempi sensibilmente più brevi, viene garantito anche l'allineamento delle performance rispetto ai sistemi primari ed esiste la possibilità di prorogare, per un tempo limitato, la disponibilità delle risorse elaborative oltre il massimo periodo di base. Vengono assicurate l'esecuzione e conservazione dei backup e la disponibilità presso il sito dei sistemi e delle configurazioni da poter utilizzare per i casi in cui si renda necessario il ripristino. Tier 3: la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare). Tier 4: la soluzione prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. Le altre caratteristiche sono quelle del Tier 3, con la possibilità di aggiornamento dei dati (RPO) con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono).

	Tier 5: la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario. Tier 6: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività in tempi molto ristretti.Le altre caratteristiche sono uguali a quelle del Tier 5.

PARTE TECNICA

PRE-REQUISITI	• Aver svolto le attività di cui ai servizi delle schede D1 e D2; • Disporre di un sito alternativo a quello di produzione (D3); • Assicurarsi i servizi di replica dati per il DR della scheda D5; • Per il tier dal 3 in poi disporre del collegamento e dei servizi di rete della scheda D6
CARATTERISTICHE TECNICHE	<u>A1 – A2 (hw e sw)</u> • Le tipologie di infrastrutture HW richieste, la loro esatta quantificazione e il dettaglio delle rispettive configurazioni sw • La tipologia e la quantiità di spazio storage richiesto per le repliche dei dati del cliente • Tutte le informazioni attinenti alla replica dei dati (modalità, frequenza, tolleranza, ecc.) o RPO (da D1 – D2) • I tempi entro cui l'infrastruttura dovrà iniziare a erogare servizi dal momento di dichiarazione della crisi o RTO (da D1 –D2) <u>A3 (postazioni)</u> • Numero di postazioni e tipologia • Disponibilità Sala/e riunione attrezzate (da sk D3 new) • Esigenze fonia
ADEMPIMENTI PREVISTI	• Installazione, manutenzione ed aggiornamento tecnologico delle infrastrutture hw, sw e delle postazioni di lavoro come da piano condiviso con il cliente • Verifica di conformità periodica delle componenti rispetto alla soluzione di DR) • Garantire il rispetto della legislazione vigente per quanto riguarda il trattamento dei dati personali o riservati della propria clientela. • Garantire il rispetto della legislazione vigente sul trattamento dei dati personali da parte degli amministratori di sistema (DLGS 196/03 all.B) e le misure minime di sicurezza • Per le licenze: vedi adempimenti non previsti
ADEMPIMENTI NON PREVISTI	• Supporto al cliente per le problematiche di tipo applicativo durante lo scenario di crisi • Durante le fasi di test di simulazione e in condizioni di esercizio in emergenza dopo la dichiarazione di disastro, si assume che le licenze del sw ripristinato presso il sito di DR siano in carico all'Amministrazione ; in caso contrario, deve esserne esplicitamente richiesto l'inserimento nel Servizio.
INDICATORI MINIMI DI SERVIZIO	• RPO e RTO compatibili con il tiee e la tipologia di soluzione scelta • % disponibilità delle infrastrutture presenti nel sito di DR nell'arco della durata del contratto • Tempi di riparazione degli eventuali guasti e di ripristino delle anomalie, sia in caso di scenario "standard" sia in caso di scenario di "crisi"; • Tempo entro il quale postazioni previste dal Servizio vengono rese disponibili .

STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Produzione di report secondo la periodicità richiesta dall'amm.ne/Ente; • Verifica di conformità periodica delle componenti e loro aggiornamento • Relazioni a seguito di operazioni di test e collaudo • Report sugli SLA

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	• Costi di investimento (HW, SW, servizi, postazioni di lavoro, telefonia e connettività dati) per la realizzazione iniziale della soluzione in base ai requirements del cliente • Eventualmente costi di gestione della soluzione per il primo anno (o porzione di anno in cui si avvia il progetto)
COSTI PERIODICI	• Canoni di gestione della soluzione (HW e SW nel caso in cui l'Amministrazione non li acquisti), manutenzioni HW, manutenzioni SW, servizi, postazioni di lavoro, canoni di telefonia e connettività dati). • Costi di gestione del contratto (fiscale, legale)
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	• Costi di investimento (HW, SW, servizi) per l'adeguamento dell'impianto iniziale a seguito di variazioni nei requirements del cliente: aumento e/o variazione dei sistemi di produzione, variazioni degli SLA richiesti dal cliente • Adeguamento dei canoni di gestione della soluzione a seguito di variazioni nei requirements del cliente: HW e SW nel caso in cui l'Amministrazione non li acquisti, manutenzioni HW, manutenzioni SW, servizi, canoni di telefonia e linee dati, costi di gestione del contratto (fiscale, legale); • Eventuale adeguamento dei costi del servizio/ dei canoni per variazioni in corso d'opera ad es. delle risorse elaborative, delle CPU, dello storage, dei TB, della connettività (vedi scheda D5), del numero di pdl necessarie

PARTE TECNICA

Sotto-servizio C. Gestione e manutenzione del sito di DR

PRE-REQUISITI	Disponibilità del sito attrezzato con aree CED
CARATTERISTICHE TECNICHE	Funzionamento e manutenzionabilità degli impianti (elettrico, condizionamento, antincendio, …)
ADEMPIMENTI PREVISTI	La gestione e manutenzione degli spazi dedicati e/o degli spazi condivisi, deve prevedere almeno le seguenti caratteristiche: • Manutenzione ordinaria/riparazione delle opere edili • Manutenzione ordinaria/riparazione degli impianti tecnologici • Assistenza tecnica per la conduzione degli impianti tecnologici compatibile con i livelli di servizio richiesti dalla soluzione di DR
ADEMPIMENTI NON PREVISTI	N.A.
INDICATORI MINIMI DI SERVIZIO	Percentuale di disponibilità dell'infrastruttura tecnologica del sito nella finestra temporale di servizio richiesta dall'Amministrazione/Ente Tempi di risposta e intervento a fronte di richieste dell'ente per la gestione del sito o la riparazione a fronte di guasti/anomalie
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report/sopralluoghi periodici sui test di verifica delle caratteristiche di ridondanza e autonomia dei sistemi di continuità elettrica e condizionamento. • Verifica della conformità e tempestività dei servizi dell'esito dei test/collaudi e periodici rispetto ai test case concordati (anche attraverso i servizi della scheda D8) • Report andamento SLA
COMPETENZE RICHIESTE	• Competenze sulle norme per l'attrezzaggio e gestione di spazi CED • Competenze sulla conduzione di impianti tecnologici • Competenze sulle soluzioni tecnologiche di disaster recovery
TEMPI DI REALIZZAZIONE	N.A.

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Non previsti
COSTI PERIODICI	• Costi a canone per la gestione e manutenzione degli spazi CED e dell'infrastruttura tecnologica • Consumi energetici in caso di sito di proprietà/gestione dell'Ente.
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali, da definire in base alle esigenze dell'Ente: Possibili costi ad hoc (una tantum) o adeguamento dei canoni di gestione e manutenzione del sito / della soluzione a seguito di variazioni dei requisiti, dei mq attrezzati, degli spazi CED, delle PdL e dell'infrastruttura tecnologica

SCHEDA SERVIZIO: D5

PARTE GENERALE

DENOMINAZIONE	D5: Servizi di replica dati per il DR
DESCRIZIONE	Il servizio di copia e trasferimento remoto a fini di backup e restore dei dati,immagine dei sistemi, applicazioni, può avvenire con modalità diverse: • trasferimento (elettronica e non) dei supporti di back up, relativa conservazione e possibilità di riconsegna • replica via rete del contenuto dei dischi
CORRISPONDENZA ITIL	Service Design – IT Service Continuity Management Service Operation
CORRISPONDENZA CPV	72910000-2
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP CON PAQ
TIER CUI SI RIFERISCE IL SERVIZIO	TIER 1, TIER 2, TIER 3, TIER 4, TIER 5, TIER 6 Tier 1: prevede l'esecuzione, il trasporto e la conservazione dei backup (di dati, applicazioni e "immagine del sistema") in un sito diverso dal primario e, per i casi in cui si renda necessario assicurare il ripristino, la disponibilità di un sito "vuoto" attrezzato, pronto a ricevere le componenti e configurazioni necessarie, ove fosse richiesto, per far fronte all'emergenza (on demand). I backup (dei dati, delle applicazioni e dell'"immagine del sistema") sono conservati presso il sito remoto. In tale sito deve essere prevista la disponibilità, in caso di emergenza, sia dello storage su disco, dove riversare i dati conservati, sia di un sistema elaborativo in grado di permettere il ripristino delle funzionalità IT. Tier 2: la soluzione è simile a quella del Tier 1, vengono assicurate l'esecuzione, il trasporto, la conservazione dei backup (dei dati, delle applicazioni e dell'"immagine del sistema") e la disponibilità presso il sito dei sistemi e delle configurazioni da poter utilizzare per i casi in cui si renda necessario il ripristino, con la differenza che le risorse elaborative possono essere disponibili in tempi sensibilmente più brevi, viene garantito anche l'allineamento delle performance rispetto ai sistemi primari. Tier 3, 4, 5 e 6: prevedono il servizio per la esecuzione e conservazione di un ulteriore copia di backup Tier 3, 4: In questi due Tier si effettua una replica asincrona dei dati a disco presso un sito secondario che ha un volume di storage equivalente a quello del sito primario. Al fine di effettuare i test presso il sito secondario è opportuno disporre di almeno una terza copia dei dati per non interrompere le repliche del sito primario. Rimane comunque buona norma trasportare in un sito diverso dal primario il backup dei dati (in modo elettronico o attraverso mezzi di trasporto convenzionali). Tier 5, 6: In questi due Tier si effettua una replica sincrona dei dati a disco presso un sito secondario che ha un volume di storage equivalente a quello del sito primario. Al fine di effettuare i test presso il sito secondario è opportuno disporre di almeno una terza copia dei dati per non interrompere le repliche del sito primario. Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario (ferma restando la necessità di non prescindere dallo specifico contesto applicativo). Rimane comunque buona norma trasportare in un sito diverso dal primario il backup dei dati

PARTE TECNICA

PRE-REQUISITI	• D1 - Consulenza per autovalutazione e predisposizione Studio di fattibilità art. 50 bis. • D2 – Servizio di predisposizione dei piani di CO/DR e progettazione organizzativa e tecnologica • D3 - Sito di Disaster Recovery: aree CED e aree Posti di Lavoro • D4 - Componenti HW e SW della soluzione di DR • Rispetto della legislazione vigente per quanto riguarda il trattamento dei dati personali (D.lgs. 196/03) e s.m.i., nonché dei provvedimenti e raccomandazioni del Garante, in particolare quelli sugli amministratori di sistema
CARATTERISTICHE TECNICHE	Il servizio di salvataggio remoto dei dati può essere previsto secondo due modalità differenti: **Modalità 1: attraverso il trasferimento dei supporti di backup,** prevedendo in questo caso la relativa conservazione dei supporti e la riconsegna dei supporti magnetici, ove richiesto. Con questo servizio il Fornitore si impegna ad effettuare il ritiro e la riconsegna dei supporti che contengono i dati di backup dei sistemi del Cliente. Il Fornitore provvederà anche al trasporto dei supporti magnetici dalla sede del Cliente sino al sito di conservazione (es.: un "caveau" di massima sicurezza) ove li custodirà per il tempo concordato nel contratto di fornitura prima di rimetterli in "rotazione ". I livelli di servizio prevedono che: • la soluzione sia di tipo "on demand" (tipicamente tier 1 - 2), con un RPO > di 24h, in funzione della frequenza di salvataggio dei dati, ed un RTO > di 24h, in funzione della disponibilità di un sito alternativo di ripristino; • il servizio di gestione, conservazione e trasporto dei supporti di backup presso il sito di conservazione può comprendere, oltre al servizio base di presa/consegna, custodia dei supporti fisici, anche le seguenti opzioni aggiuntive: a. Gestione in "rastrelliera" dedicata con supporto sw di management b. Riconsegna supporti in emergenza in orario di lavoro c. Riconsegna supporti in emergenza fuori dal normale orario di lavoro **Modalità 2: attraverso la replica del contenuto dei dischi via rete (tier 3,4,5 e 6).** Il servizio prevede la disponibilità di procedure e sistemi per la creazione di una o più copie dei dati di produzione. Tale modalità prevede che le copie dei dati siano trasferite via rete presso il sito di DR e lì custodite. E' richiesto che le procedure e i sistemi di copia dei dati siano costantemente attivi e in grado di trasferire ogni aggiornamento del singolo dato dal sito primario al sito di DR in modalità sincrona o asincrona. La disponibilità della copia dei dati via rete può essere assicurata attraverso il servizio di housing delle risorse con copia sincrona, asincrona, continua, tramite uso di linee dedicate tra i due siti. Le risorse a supporto della movimentazione dei dati (es. storage e connettività) devono essere incluse nel servizio in modalità dedicata (sempre attive a supporto della copia dei dati, secondo livelli di servizio prestabiliti). Per queste risorse dedicate, è possibile richiedere anche il solo servizio di housing, senza approvvigionamento delle risorse dedicate in carico al fornitore (in tal caso, l'acquisizione è in carico all'Amministrazione). Il servizio può includere attività di controllo e gestione della copia / replica dei dati in carico al fornitore.
ADEMPIMENTI PREVISTI	**<u>Modalità 1</u>** ***1. Procedura di presa e consegna con trasporto tradizionale:*** • copia multipla • presa e consegna giornaliera di una o più box con n.ro cartucce o nastri variabile

	• definizione del luogo di prelievo / consegna • definizione giorni e orari di prelievo / consegna • definizione modalità di conservazione presso il sito di stoccaggio (box, valige, rastrelliere) • definizione distanza minima del sito di stoccaggio dal sito di produzione dei nastri • definizione delle modalità, tempi, luogo e fascia oraria di consegna di nastri / box / valige stoccate • definizione delle modalità di consegna urgente in situazione di disastro (luogo, fascia oraria di accettazione della richiesta, modalità di richiesta) ***Mezzi di trasporto adibiti al prelievo consegna:*** • caratteristiche e numerosità • misure di sicurezza adottate • numero minimo di persone addetto per ciascun veicolo. **<u>Modalità 2</u>** • **Tier 3** - **Tier 4** - Il Servizio prevede di disporre delle risorse elaborative e storage presso il sito di DR installate e attive, dedicate, specificamente al supporto della movimentazione dei dati; è richiesta la disponibilità di programmi appositi oppure tramite feature hw dei sistemi storage in grado di attivarsi ad ogni modifica del singolo dato in ambiente di produzione e di prelevare, trasferire e applicare una copia del dato modificato sullo storage remoto via rete. L'utente solitamente non ha accesso diretto ai dati copiati, ma questi possono essere utilizzati presso il sito di DR in caso di disastro. Il trasferimento è eseguito in modalità asincrona: ciò significa che l'applicazione che esegue la modifica del dato tiene conto dei *soli* aggiornamenti in ambiente di produzione (e non attende conferma di aggiornamento dallo storage di DR). • **Tier 5 e 6** - Il Servizio prevede di disporre delle risorse elaborative e storage presso il sito di DR installate e attive, dedicate, specificamente al supporto della movimentazione dei dati; è richiesta la disponibilità di programmi appositi oppure tramite feature hw in grado di attivarsi ad ogni modifica del singolo dati in ambiente di produzione e di prelevare, trasferire e applicare una copia del dato sullo storage remoto via rete. L'utente solitamente non ha accesso diretto ai dati copiati, ma queste possono essere utilizzate presso il sito di DR in caso di disastro. Il trasferimento è eseguito in modalità sincrona: ciò significa che l'applicazione che esegue la modifica del dato tiene conto sia della conferma di aggiornamento in ambiente di produzione sia della conferma dall'ambiente di DR.
ADEMPIMENTI NON PREVISTI	Supporto al cliente per le problematiche di tipo applicativo durante lo scenario di crisi
INDICATORI MINIMI DI SERVIZIO	**<u>Modalità 1</u>** • Tempi di ritiro/consegna • Misure di sicurezza per il trasporto **<u>Modalità 2</u>** • RPO
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	**<u>Modalità 1</u>** • Sopralluoghi per verificare che la conservazione avvenga secondo modalità e in luogo sicuro • Livello di sicurezza dei mezzi di trasporto. • Simulazioni per verificare la prontezza del servizio di trasporto, quando richiesta. **<u>Modalità 2</u>** • Esito di operazioni di test e collaudo • Report sull'RPO e gli altri SLA richiesti
COMPETENZE RICHIESTE	• Competenze sulle principali norme e standard riferiti alla copia e conservazione

	dei dati per il DR • Competenze sulle varie soluzioni tecnologiche previste per le soluzioni di copia e conservazione dei dati per il disaster recovery
TEMPI DI REALIZZAZIONE (ELAPSED)	**Modalità 1** • Piccola Amministrazione: 1-2 mesi solari • Media Amministrazione: 1-2 mesi solari • Grande Amministrazione: 2-3 mesi solari • Grandissima Amministrazione: 3-4 mesi solari **Modalità 2** • Piccola Amministrazione: 2-4 mesi solari • Media Amministrazione: 4-6 mesi solari • Grande Amministrazione: 6-8 mesi solari • Grandissima Amministrazione: 8-12 mesi solari

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	**Modalità 1** • Costi correlati alla creazione di backup su supporti fisici (es. acquisizione supporti fisici) ed all'allestimento del sito di stoccaggio. **Modalità 2** **Opzione a)** • Costi correlati agli investimenti per l'acquisizione sistemi delle infrastrutture e dei sistemi, ove previsti, a supporto della replica (se non sono inclusi nel servizio) • Eventualmente costi di gestione della soluzione per il primo anno (o porzione di anno in cui si avvia il progetto)
COSTI PERIODICI	Costi per il servizio di trasferimento/conservazione dei supporti Costi per i servizi di copia inclusi nei canoni di gestione e mantenimento della soluzione (HW e SW nel caso in cui non siano di proprietà dell'Amministrazione). Costi di gestione del contratto (fiscale, legale)
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Costi di investimento per l'adeguamento dei sistemi/procedure per la produzione dei backup Costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA
Sotto-servizio D. Disponibilità di spazi ad uso ufficio destinati ad ospitare le PdL

PRE-REQUISITI	Disponibilità di spazi da attrezzare ad uso ufficio per ospitare le Postazioni di Lavoro per il personale autorizzato dall'Ente
CARATTERISTICHE TECNICHE	Fornitura di spazi ad uso ufficio, presso il sito di DR o presso altro sito idoneo concordato, che possono essere: • **dedicati**: fornitura di specifici spazi concordati con l'Amministrazione che soddisfino i requisiti progettuali. L'area sarà dedicata in maniera univoca all'Amministrazione • **condivisi**: fornitura di spazi che rispondano alle specifiche progettuali, ma che possono ospitare apparati e sistemi condivisibili anche con altri Enti o Clienti Le macro aree che devono essere considerate per determinare l'idoneità del sito sono: SICUREZZA FISICA - distanza dal DC primario o dalle sedi locali di lavoro, tale da soddisfare la protezione dagli scenari di disastro identificati in fase di Studio di Fattibilità - dotazione di misure tecnologiche e procedurali di sicurezza fisica idonee a proteggerlo da intrusioni dall'esterno (sicurezza perimetrale) o da accessi di

	persone non autorizzate alle aree riservate (stanze uffici, vani tecnici) - dispositivi di prevenzione, rilevamento e segnalazione contro il pericolo di incendio <u>SERVIZI LOGISTICI</u> - presidio e controllo accessi h24 - sala riunioni attrezzata con video proiettore e teleconferenza - servizi di telefonia anche IP - gestione ricevimento e stoccaggio apparati - raggiungibilità e mezzi di trasporto - aree interne di ristoro - strutture ricettive alberghiere e ristorazione in zona <u>AFFIDABILITÀ INFRASTRUTTURE TECNOLOGICHE</u> - ridondanza sistemi di continuità elettrica - ridondanza sistemi di condizionamento Le caratteristiche ed i requisiti generali sono riportati nella scheda D2 e servono da riferimento durante la progettazione esecutiva.
ADEMPIMENTI PREVISTI	• Possesso dei titoli autorizzativi previsti dalle leggi e regolamenti vigenti all'atto della verifica di idoneità del sito • Certificazione periodica degli impianti tecnologici (elettrico, condizionamento, rilevazione fumi, antincendio, sicurezza) • Attuazione del processo di gestione degli accessi del personale e anti-intrusione del sito
ADEMPIMENTI NON PREVISTI	• Connettività WAN-SPC • Modifiche agli impianti tecnologici non conseguenti alla normale attività di manutenzione ordinaria o di riparazione • Esecuzione degli interventi individuati come propedeutici sul sito principale per renderlo conforme ai requisiti definiti nei servizi della scheda D2 come passo propedeutico/prerequisito della realizzazione della soluzione di DR
INDICATORI MINIMI DI SERVIZIO	• Tempi di messa a disposizione a partire dal momento della richiesta dell'Ente secondo i valori richiesti dall'Ente • Percentuale di disponibilità degli spazi attrezzati per le PdL nella finestra temporale di servizio richiesta dall'Amministrazione/Ente
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Documentazione attestanti la conformità ai requisiti e titoli autorizzativi • Sopralluoghi di verifica delle caratteristiche di ridondanza e autonomia dei sistemi di continuità elettrica e condizionamento. • Verifica del rispetto delle misure di sicurezza fisica e dei servizi logistici richiesti.
COMPETENZE RICHIESTE	• Competenze sulle norme per l'attrezzaggio e gestione di spazi ad uso ufficio • Competenze impianti tecnologici • Competenze sulle soluzioni tecnologiche di disaster recovery
TEMPI DI REALIZZAZIONE	N.A.

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	• Costi di investimento per opere di adeguamento locali e servizi logistici richiesti dall'Amministrazione • Eventuali costi non standard dovuti alla fase di startup della soluzione
COSTI PERIODICI	• Costi a canone per l'uso dei locali ufficio (affitto dei locali, consumi, sorveglianza, oneri contrattuali)
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	• Eventuali costi di investimento per opere di adeguamento locali, servizi logistici a seguito di variazioni delle esigenze dell'Ente, quali ad esempio: incremento degli spazi richiesti, variazioni dei SLA • Adeguamento dei canoni per l'uso dei locali uso ufficio dovuto ad incrementi dei costi per i consumi operato dal Fornitore delle utility pubbliche

PARTE TECNICA

Sotto-servizio E. Gestione e manutenzione degli spazi ad uso ufficio per ospitare le PdL

PRE-REQUISITI	Disponibilità del sito attrezzato con aree CED
CARATTERISTICHE TECNICHE	Verifica e certificazione periodica della conformità del servizio e dell'esecuzione dei test di funzionalità degli impianti (elettrico, condizionamento, antincendio, …)
ADEMPIMENTI PREVISTI	La gestione e manutenzione degli spazi dedicati e/o degli spazi condivisi, deve prevedere almeno: • Manutenzione ordinaria/riparazione delle opere edili • Manutenzione ordinaria/riparazione degli impianti tecnologici • Presidio h24 per la conduzione degli impianti tecnologici Le operazioni di manutenzione ordinaria devono essere in linea con gli SLA.
ADEMPIMENTI NON PREVISTI	N.A.
INDICATORI MINIMI DI SERVIZIO	• Percentuale di disponibilità degli spazi ad uso ufficio per ospitare le PdL • Tempestività della disponibilità degli spazi secondo i tempi definiti dall'ente • Tempi di risposta e intervento a fronte di richieste dell'ente
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report/sopralluoghi periodici sui test di verifica delle caratteristiche di ridondanza e autonomia dei sistemi di continuità elettrica e condizionamento. • Verifica della conformità e tempestività dei servizi e dell'esito dei test di collaudo e periodici rispetto ai test case concordati • Report andamento SLA
COMPETENZE RICHIESTE	• Competenze sulle norme per l'attrezzaggio e gestione di spazi uso ufficio • Competenze sulla conduzione di impianti tecnologici • Competenze sulle soluzioni tecnologiche di disaster recovery
TEMPI DI REALIZZAZIONE	N.A.

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Non previsti
COSTI PERIODICI	Costi a canone per la gestione e manutenzione degli spazi uso ufficio e dell'infrastruttura tecnologica
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali, da definire in base alle esigenze dell'Ente Possibili costi ad hoc (una tantum) o adeguamento dei canoni di gestione e manutenzione del sito / della soluzione a seguito di variazioni dei requisiti progettuali (es. per l'incremento degli spazi da adibire a uso ufficio

SCHEDA SERVIZIO: D6

PARTE GENERALE

DENOMINAZIONE	D6: Servizi di rete per il DR
DESCRIZIONE	Progettazione, realizzazione, gestione e manutenzione delle componenti di rete necessarie per la soluzione di DR. Il servizio si articolerà nei seguenti sottoservizi: A. Progettazione e dimensionamento della soluzione di rete; B. Fornitura, manutenzione e gestione, anche in modalità condivisa tra più amministrazioni, dei componenti di rete della soluzione di DR, inclusi quelli necessari alla gestione dell'instradamento alternativo degli accessi dalla periferia in caso di emergenza
CORRISPONDENZA ITIL	Service Design – IT Service Continuity Management Service Operation
CORRISPONDENZA CPV	Sottoservizio A): 72510000-3 Sottoservizio B): 72720000-3, 72510000-3, 72511000-0 e 72514100-2
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP CON PAQ
TIER CUI SI RIFERISCE IL SERVIZIO	TIER 1, TIER 2, TIER 3, TIER 4, TIER 5, TIER 6 **Tier 1 e 2:** non ci sono collegamenti di rete fra siti (primario e di DR); relativamente solo ai collegamenti di rete tra il sito di DR e l'utenza periferica possono essere previsti i sottoservizi A e B; **Tier 3, 4, 5 e 6:** prevedono collegamenti di rete fra i siti (primario e di DR) e tra il sito di DR e l'utenza periferica; per entrambe le tiplogie di rete sono previsti i sottoservizi A e B; o Tier 3: la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare). o Tier 4: la soluzione prevede che le risorse elaborative garantite, coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. Le altre caratteristiche sono quelle del Tier 3, con la possibilità di aggiornamento dei dati (RPO) con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono). o Tier 5: la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario. o Tier 6: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario,

	rendendo così possibile ripristinare l'operatività in tempi molto ristretti.Le altre caratteristiche sono uguali a quelle del Tier 5.

PARTE TECNICA
Sotto-servizio A: Progettazione della soluzione di rete

PRE-REQUISITI	• D1: Consulenza per autovalutazione e predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4 dell'art. 50 bis del CAD • D2 – Servizio di predisposizione dei piani di CO/DR e progettazione organizzativa e tecnologica della soluzione di DR (sottoservizi B e D) da svolgere o parallelamente o con verifica delle relative interazioni; • D3 - Sito di Disaster Recovery: aree CED e aree attrezzate per i posti di lavoro • D4 - Componenti HW e SW della soluzione di DR • D5 – Servizi di replica dati
CARATTERISTICHE TECNICHE	Progettazione e dimensionamento della soluzione di rete articolata, a seconda del tier, nei seguenti ambiti: 1. Componenti di rete (collegamenti ed apparati) necessari a collegare, anche in modo ridondato, il sito primario, il sito/i siti di DR e la rete periferica; 2. Componenti di rete e della soluzione per l'instradamento alternativo, in caso di emergenza, tra il sito secondario di DR e la rete periferica; 3. Modalità di gestione e manutenzione della soluzione di rete di DR
ADEMPIMENTI PREVISTI	Il sotto-servizio di progettazione prevede le seguenti macro-attività: • *High Level Design* (Progetto Generale), che prevede i seguenti ambiti ed attività: 1. Raccolta e analisi dei requisiti 2. Progettazione, in eventuale modalità ridondata, dei seguenti strati della rete primaria e dei relativi aspetti di sicurezza: o Fisica o Trasporto o Switching/Routing Nel caso dei Tier 5 e 6, dovendosi prevedere un collegamento di tipo "sincrono", la progettazione della rete del DR dovrà tener conto della distanza massima tra sito primario e sito secondario; 3. Progettazione della rete secondaria per l'instradamento alternativo (satellitare, ponte radio, Wimax, Wi-Fi, mobile, ecc...) e dei relativi aspetti di sicurezza; 4. Progettazione della soluzione di gestione e delle relative funzionalità in grado di garantire la gestione centralizzata della rete di DR; 5. Progettazione degli interventi di adeguamento degli ambienti che dovranno ospitare gli apparati e dei relativi aspetti di sicurezza; 6. Cronoprogramma delle attività da concordare tra committente e fornitore. • *Low Level Design* (Progetto di Dettaglio), che prevede le seguenti attività e deliverable: 1. Rete Primaria o Sopralluoghi dei siti cliente (anche sotto il profilo della sicurezza) o Progetto esecutivo (link design) 2. Apparati o Sopralluoghi dei siti cliente (anche sotto il profilo della sicurezza) o Progetto esecutivo (link budget) o Progetto di adeguamento siti 3. Rete secondaria per l'instradamento alternativo o Sopralluoghi o Progetto esecutivo (link budget) o Progetto di adeguamento siti 4. Definizione delle modalità operative per le procedure di gestione o Analisi requisiti

	o Pianificazione e progettazione processi 5. Gestione della soluzione di rete del DR o Definizione delle funzionalità e dei requisiti tecnici o Progetto esecutivo 6. Collaudo o Piano di collaudo 7. Piano complessivo di progetto 8. Metodologia di Project Management
ADEMPIMENTI NON PREVISTI	• Attività operative di PM, procurement materiali, adeguamento siti, installazione, posa in opera, collaudo e formazione • Attività riguardanti l'ottenimento dei permessi necessari alle attività di scavo e/o al rilascio delle frequenze
INDICATORI MINIMI DI SERVIZIO	• Completezza • Rispetto dei Tempi pianificati Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Governance e reporting dei lavori, rispetto del piano di attività • Documentazione attestanti la conformità ai requisiti e titoli autorizzativi • Possesso delle competenze professionali richieste (vedi sotto)
COMPETENZE RICHIESTE	• Competenze sulle principali norme e standard riferiti alle TLC, al DR ed alla sicurezza • Competenze sulle norme per l'attrezzaggio e la gestione di siti per le telecomunicazioni • Competenze tecnologiche previste per le varie soluzioni di rete per il DR
TEMPI DI REALIZZAZIONE	Piccola Amministrazione o Effort : 60-90 gg/u professionali o Elapsed : 1-2 mesi solari Media Amministrazione o Effort : 90-150 gg/u professionali o Elapsed : 2-3 mesi solari Grande Amministrazione o Effort : 150-210 gg/u professionali o Elapsed : 3-4 mesi solari Grandissima Amministrazione o Effort : 210-240 gg/u professionali o Elapsed : 5-6 mesi solari

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Valutabile in numero di giornate/uomo professionali per tariffa professionale di tipo Senior.
COSTI PERIODICI	NA
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	A consumo in funzione dei profili professionali richiesti e del maggior effort per eventuali extracosti necessari al reperimento di eventuali dati necessari alla progettazione. Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA

Sotto-servizio B: Fornitura, manutenzione e gestione, anche in modalità condivisa tra più amministrazioni, dei componenti di rete della soluzione di DR, inclusi quelli necessari alla gestione dell'instradamento alternativo degli accessi dalla periferia in caso di emergenza

PRE-REQUISITI	D1: Consulenza per autovalutazione e predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4 dell'art. 50 bis del CAD D2 – Servizio di predisposizione dei piani di CO/DR e progettazione organizzativa e tecnologica della soluzione di DR D5 - Servizi di rete e di copia per il DR: Sottoservizio A (Progettazione della soluzione di rete) D3 - Sito di Disaster Recovery: aree CED e aree Posti di Lavoro D4 - Componenti HW e SW della soluzione di DR
CARATTERISTICHE TECNICHE	**Tier 1 e 2**: Non è previsto alcun collegamento di rete tra sito di DR e sito primario; Possono essere previsti collegamenti non ridondati, tra sito di DR ed utenza periferica (interna ed esterna); **Tier 3**: E' previsto un collegamento di rete, anche non ridondato, tra sito di DR e sito primario; Sono previsti collegamenti, anche non ridondati, tra sito di DR ed utenza periferica (interna ed esterna); **Tier 4**: E' previsto un collegamento di rete ridondato tra sito di DR e sito primario; Sono previsti collegamenti di rete ridondati tra sito di DR ed utenza periferica (interna ed esterna); **Tier 5 e 6**: E' previsto un collegamento di rete ridondato e per l'instradamento alternativo tra sito di DR e sito primario; Sono previsti collegamenti di rete ridondati e per l'instradamento alternativo tra sito di DR ed utenza periferica(interna ed esterna);
ADEMPIMENTI PREVISTI	Fatta salva la preventiva verifica circa la disponibilità di eventuali convenzioni/accordi quadro per la PA (es.SPC), il sotto-servizio B, a seconda dei vari tier, prevederà in parte o tutte le seguenti attività: 1. Rete Primaria • Sopralluoghi • Gestione amministrativa dei permessi • Procurement fibra o altra tipologia di connettività (rame, satellitare, ponte radio, ecc...) • Installazione e posa in opera (opere civili e collaudo) 2. Apparati • Sopralluoghi • Predisposizione siti • Procurement apparati TLC, stazioni di energia e sistemi di gestione • Collaudo in fabbrica • Installazione e messa in opera centro di gestione (configurazione e collaudo) • Installazione e messa in opera apparati (configurazione, presa in carico dal centro di gestione e collaudo) 3. Rete secondaria per l'instradamento alternativo • Sopralluoghi • Predisposizione siti • Procurement apparati per l'instradamento alternativo (satellitare, ponte radio, mobile, ecc...), stazioni di energia e centro di gestione • Collaudo in fabbrica • Installazione e messa in opera centro di gestione (configurazione e collaudo) • Installazione e messa in opera apparati (configurazione, presa in carico dal centro di gestione e collaudo) 4. Collaudo di sistema

	5. Manutenzione delle componenti di rete • Help Desk • Correttiva • Preventiva 6. Gestione delle componenti di rete • Presidio I sistemi di gestione delle varie tipologie di apparati, da prevedersi in modalità ridondata (sito primario e sito di DR), dovranno permettere l'effettuazione di attività di pianificazione, installazione, gestione, manutenzione e fornitura di reti e servizi di telecomunicazioni e dovranno essere funzionalmente strutturati secondo il modello a livelli presentato nella raccomandazione ITU-T di riferimento. I sistemi di gestione, infine, dovranno essere in grado di fornire funzionalità di provisioning di link e di circuito end-to-end e allarmistica integrata, attraverso un' integrazione con un livello di Network Management superiore basata su interfaccia standard (ad es. Solution Set for the Multi-Technology Network Management NML-EML Interface), che dovrà risiedere in un apposito centro servizi TLC o NOC (Network Operating Center) eventualmente da prevedersi in modalità "service" (nel caso di piccole e medie amministrazioni) o dedicata (nel caso di aggregati di piccole/medie amministrazioni, di grandi e di grandissime amministrazioni). Il NOC ha l'obiettivo di garantire la gestione integrata di tutti i sistemi di TLC dell'Amministrazione oggetto di fornitura per erogare almeno i seguenti servizi: • Fault Management • Configuration Management • Performance Management • Administration Management • Security Management Il sottoservizio prevede anche la fornitura di personale, eventualmente presso il cliente, specializzato in ambito TLC e DR al fine di supportarlo nelle attività di: • Supervisione, monitoraggio e gestione della soluzione di rete del DR • Condivisione con il cliente della procedura operativa, in caso di scenario di crisi, delle attività a carico del fornitore e l'output desiderato • Collaudi periodici con relativa certificazione fornitore ed utente (relativo alla soluzione di rete) • Gestione del trattamento dei dati personali da parte degli amministratori di sistema, e nel rispetto del DLGS 196/03 all.B, direttiva 95/46/CE del 24/5/12 s.m.i. e successivi provvedimenti del Garante della Privacy, incluse le raccomandazioni e provvedimenti sull'uso delle soluzioni "cloud")
ADEMPIMENTI NON PREVISTI	Supporto al cliente per le problematiche di tipo applicativo durante lo scenario di crisi.
INDICATORI MINIMI DI SERVIZIO	• RPO e RTO compatibili con la tipologia di soluzione scelta • % di alcuni parametri nell'arco della durata del contratto (disponibilità collegamenti, tasso di errore, tempo di latenza, jitter, ecc...) • Tempi di ripristino delle anomalie che impattano sull'erogazione del servizio, sia in caso di scenario "standard" sia in caso di scenario di "crisi" (possono essere concordati anche 2 SLA differenti) • Tempo entro il quale avviene la commutazione tra il centro primario ed il centro di DR e/o tempo entro il quale la periferia è in grado di attestarsi sul centro di DR
STRUMENTI DI VERIFI-CA DELLA CONFOR-MITA' DEL SERVIZIO	• Produzione di certificazioni • Relazioni a seguito di operazioni di test e collaudo • Report sugli SLA
COMPETENZE RICHIESTE	• Competenze sulle principali norme e standard riferiti alle TLC ed al DR • Competenze sulle norme per l'attrezzaggio e la gestione di siti per le telecomunicazioni • Competenze tecnologiche previste per le varie tipologie di soluzioni di rete per il DR

TEMPI DI REALIZZAZIONE (ELAPSED)	• Piccola Amministrazione: 2-4 mesi solari • Media Amministrazione: 4-6 mesi solari • Grande Amministrazione: 6-8 mesi solari • Grandissima Amministrazione: 8-12 mesi solari

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Costi correlati agli investimenti per la realizzazione iniziale della soluzione in base ai requirements del cliente Eventualmente costi di gestione della soluzione per il primo anno (o porzione di anno in cui si avvia il progetto)
COSTI PERIODICI	Canoni di mantenimento e di gestione della soluzione (HW e SW nel caso in cui l'Amministrazione non li acquisti), manutenzioni HW, manutenzioni SW ed altri eventuali servizi). Costi di gestione del contratto (fiscale, legale) Costi di ammortamento delle infrastrutture
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Costi di investimento per l'adeguamento dell'impianto iniziale a seguito di variazioni nei requirements del cliente: aumento e/o variazione dei sistemi di produzione, variazioni degli SLA richiesti dal cliente Adeguamento dei canoni di mantenimento e gestione della soluzione a seguito di variazioni nei requirements del cliente Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

SCHEDA SERVIZIO:D7

PARTE GENERALE

DENOMINAZIONE	D**7** – Servizi di gestione della soluzione di DR sia in condizioni di normalità che in condizioni di emergenza
DESCRIZIONE	Il servizio deve assicurare la gestione ottimale della soluzione di DR al fine di assicurarne la piena efficienza. Il servizio potrà essere suddiviso in due sotto servizi: A. gestione della soluzione durante la normale operatività B. gestione dell'emergenza
CORRISPONDENZA ITIL	IT Service Continuity Management
CORRISPONDENZA CPV	72150000-1 72514000-1
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP CON PAQ
TIER CUI SI RIFERISCE IL SERVIZIO	4 – 5 – 6 Tier 4: la soluzione prevede il trasferimento dei dati dal sito primario a quello di DR attraverso un collegamento di rete tra i due siti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare) e prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. L'aggiornamento dei dati (RPO) può avvenire con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono).

	Tier 5: la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario. Tier 6: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività in tempi molto ristretti.Le altre caratteristiche sono uguali a quelle del Tier 5.

PARTE TECNICA

Sottoservizio A: Gestione della soluzione di DR in condizioni di normalità

PRE-REQUISITI	D1: Consulenza per autovalutazione e predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4 dell'art. 50 bis del CAD D2 – Servizio di predisposizione dei piani di CO/DR e progettazione organizzativa e tecnologica della soluzione di DR D3 - Sito di Disaster Recovery: aree CED e aree attrezzate per i posti di lavoro D4 - Componenti HW e SW della soluzione di DR Ove esistano contratti di ousourcing che affidino a fornitori diversi le attività di replica, copia dati e quelle di gestione della soluzione di DR e "restore" dei dati è necessario definire in entrambi gli strumenti negoziali che regolano i rapporti, il regime di responsabilità e i termini e le modalità che assicurino la corretta gestione del Sistema Informativo e che le attività di replica, copia e restore vadano a buon fine (vedi capitolo 6 delle Linee Guida, in particolare il punto 6.3.1.)
CARATTERISTICHE TECNICHE	Il fornitore dovrà eseguire tutte le attività necessarie ad assicurare che i presupposti per rispettare i valori di RPO e RTO, congruenti col tier scelto dall'Ammne/Ente, siano soddisfatti. Il servizio è un servizio prettamente informatico di gestione e verifica che i requisiti definiti dal progetto della soluzione di DR siano sempre soddisfatti e di esecuzione di interventi mirati al ripristino dei requisiti in caso di inosservanza degli stessi.
ADEMPIMENTI PREVISTI	Gli adempimenti previsti sono individuati e specificati attraverso i deliverable della scheda D2 (Progetto di DR; Piani di CO/DR) nonché nel contratto definito dall'Amne/Ente verso il fornitore In particolare, il sottoservizio D2.E deve indicare le procedure da seguire per assicurare il rispetto dei requisiti individuati. Tipicamente nel caso di replica sincrona/asincrona dei dati dovrà essere eseguito il monitoraggio della replica al fine di verificare che la stessa non venga interrotta. La corretta esecuzione di questa attività è il prerequisito per rispettare l'RPO definito nella BIA e nel progetto di DR
ADEMPIMENTI NON PREVISTI	Attività al di fuori di quelle identificate dalla scheda D2(Progetto di DR; Piani di CO/DR) nonché nel contratto definito dall'Amne/Ente verso il fornitore
INDICATORI MINIMI DI SERVIZIO	Tempestività: rispetto dei termini previsti per le attività e gli adempimenti Completezza delle attività e degli adempimenti Garanzia che sia assicurato l'RTO e l'RPO definito (a sec. del tier scelto dall'Amm.me/Ente) Numero di scostamenti oltre il valore di soglia degli elementi messi sotto controllo

STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	Verifica periodica attraverso report, riunioni periodiche verbalizzate e test verifiche a campione della conformità degli adempimenti ai termini e SLA definiti Attività di verifica della scheda D8
COMPETENZE RICHIESTE	Possesso di skill, certificazioni e possibilità di erogare il servizio h24 7x7 Competenze sulle principali norme e standard riferiti alle TLC, al DR ed alla sicurezza
TEMPI DI REALIZZAZIONE	N.A. il servizio va erogato per la durata prevista nel contratto che affida al fornitore il servizio stesso in linea con i requisiti del progetto e dei piani di CO/DR

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Solitamente nella prassi più diffusa nessuno, salvo che il servizio non sia richiesto come a consumo, allora potrà comportare costi una tantum, e andrà pagato sulla base del numero effetivo di gg.pe utilizzati e della professionalità (e tariffa) richiesta
COSTI PERIODICI	canone
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali costi derivanti da variazioni in corso d'opera o incremento/modifica degli SLA previsti, da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio o incrementando il canone o a consumo, sulla base del numero effettivo di gg.pe utilizzati e della professionalità (e tariffa) richiesta

PARTE TECNICA

Sottoservizio B gestione dell'emergenza

PRE-REQUISITI	D1: Consulenza per autovalutazione e predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4 dell'art. 50 bis del CAD D2 – Servizio di predisposizione dei piani di CO/DR e progettazione organizzativa e tecnologica della soluzione di DR D3 - Sito di Disaster Recovery: aree CED e aree attrezzate per i posti di lavoro D4 - Componenti HW e SW della soluzione di DR Ove esistano contratti di ousourcing che affidino a fornitori diversi le attività di replica, copia dati e quelle di gestione della soluzione di DR e "restore" dei dati è necessario definire in entrambi gli strumenti negoziali che regolano i rapporti, il regime di responsabilità e i termini e le modalità che assicurino la corretta gestione del Sistema Informativo e che le attività di replica, copia e restore vadano a buon fine (vedi capitolo 6 delle Linee Guida, in particolare il punto 6.3.1.)
CARATTERISTICHE TECNICHE	Esecuzione di tutte le attività, informatiche e non, per attivare l'erogazione dei servizi all'utente finale da parte del sito secondario a fronte del verificarsi di un disastro.
ADEMPIMENTI PREVISTI	Esecuzione di tutte le attività previste dalla scheda D2, dalla progettazione della soluzione (Progetto di DR), dai Piani di CO/DR, nonché nel contratto definito dall'Amne/Ente verso il fornitore, a fronte della dichiarazione del disastro.
ADEMPIMENTI NON PREVISTI	Attività al di fuori di quelle identificate dalla scheda D2(Progetto di DR; Piani di CO/DR) nonché nel contratto definito dall'Amne/Ente verso il fornitore
INDICATORI MINIMI DI SERVIZIO	Tempestività: rispetto dei termini previsti per le attività e gli adempimenti Completezza delle attività e degli adempimenti

	Garanzia che sia assicurato l'RTO e l'RPO definito (a sec. del tier scelto dall'Amm.me/Ente)
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	Verifica del rispetto del dettato contrattuale, Verifica del rispetto dei tempi di attivazione del personale del fornitore, Verifica del rispetto dei tempi di ripartenza/ripristino e della consistenza dei dati
COMPETENZE RICHIESTE	Conoscenze specifiche degli ambienti da gestire e disponibilità ad intervenire h24 7x7 su richiesta. Competenze sulle principali norme e standard riferiti alle TLC, al DR ed alla sicurezza
TEMPI DI REALIZZAZIONE	La durata del singolo intervento deve rientrare nei requisiti di RTO definito. Il servizio va erogato per la durata prevista nel contratto che affida al fornitore il servizio stesso in linea con i requisiti del Progetto e dei Piani di CO/DR

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Solitamente nella prassi più diffusa nessuno, salvo che il servizio non sia richiesto come a consumo, nel qual caso potrà comportare costi una tantum, e andra' pagato sulla base del numero effettivo di gg.pe utilizzati e della professionalità (e tariffa) richiesta
COSTI PERIODICI	Se previsto contrattualmente, a canone; si possono avere risparmi sul costo per la gestione con soluzioni c.d. di alta affidabilità tipiche dei tier 5 e soprattutto 6 che prevedono il ripristino automatico delle applicazioni sul sito di DR, in caso di indisponibilità del sito primario
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Eventuali costi derivanti da variazioni in corso d'opera o incremento/modifica degli SLA previsti, da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio o incrementando il canone o a consumo, sulla base del numero effettivo di gg.pe utilizzati e della professionalità (e tariffa) richiesta

SCHEDA SERVIZIO: D6

PARTE GENERALE

DENOMINAZIONE	D6: Servizi di rete per il DR
DESCRIZIONE	Progettazione, realizzazione, gestione e manutenzione delle componenti di rete necessarie per la soluzione di DR. Il servizio si articolerà nei seguenti sottoservizi: C. Progettazione e dimensionamento della soluzione di rete; D. Fornitura, manutenzione e gestione, anche in modalità condivisa tra più amministrazioni, dei componenti di rete della soluzione di DR, inclusi quelli necessari alla gestione dell'instradamento alternativo degli accessi dalla periferia in caso di emergenza
CORRISPONDENZA ITIL	Service Design – IT Service Continuity Management Service Operation
CORRISPONDENZA CPV	Sottoservizio A): 72510000-3 Sottoservizio B): 72720000-3, 72510000-3, 72511000-0 e 72514100-2
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP CON PAQ
TIER CUI SI RIFERISCE IL SERVIZIO	TIER 1, TIER 2, TIER 3, TIER 4, TIER 5, TIER 6 **Tier 1 e 2:** non ci sono collegamenti di rete fra siti (primario e di DR); relativamente solo ai collegamenti di rete tra il sito di DR e l'utenza periferica possono essere previsti i sottoservizi A e B; **Tier 3, 4, 5 e 6:** prevedono collegamenti di rete fra i siti (primario e di DR) e tra il sito di DR e l'utenza periferica; per entrambe le tiplogie di rete sono previsti i sottoservizi A e B; o Tier 3: la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare). o Tier 4: la soluzione prevede che le risorse elaborative garantite, coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. Le altre caratteristiche sono quelle del Tier 3, con la possibilità di aggiornamento dei dati (RPO) con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono). o Tier 5: la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario. o Tier 6: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività in tempi molto ristretti.Le altre

	caratteristiche sono uguali a quelle del Tier 5.

PARTE TECNICA
Sotto-servizio A: Progettazione della soluzione di rete

PRE-REQUISITI	• D1: Consulenza per autovalutazione e predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4 dell'art. 50 bis del CAD • D2 – Servizio di predisposizione dei piani di CO/DR e progettazione organizzativa e tecnologica della soluzione di DR (sottoservizi B e D) da svolgere o parallelamente o con verifica delle relative interazioni; • D3 - Sito di Disaster Recovery: aree CED e aree attrezzate per i posti di lavoro • D4 - Componenti HW e SW della soluzione di DR • D5 – Servizi di replica dati
CARATTERISTICHE TECNICHE	Progettazione e dimensionamento della soluzione di rete articolata, a seconda del tier, nei seguenti ambiti: 4. Componenti di rete (collegamenti ed apparati) necessari a collegare, anche in modo ridondato, il sito primario, il sito/i siti di DR e la rete periferica; 5. Componenti di rete e della soluzione per l'instradamento alternativo, in caso di emergenza, tra il sito secondario di DR e la rete periferica; 6. Modalità di gestione e manutenzione della soluzione di rete di DR
ADEMPIMENTI PREVISTI	Il sotto-servizio di progettazione prevede le seguenti macro-attività: • *High Level Design* (Progetto Generale), che prevede i seguenti ambiti ed attività: 1.Raccolta e analisi dei requisiti 2.Progettazione, in eventuale modalità ridondata, dei seguenti strati della rete primaria e dei relativi aspetti di sicurezza: o Fisica o Trasporto o Switching/Routing Nel caso dei Tier 5 e 6, dovendosi prevedere un collegamento di tipo "sincrono", la progettazione della rete del DR dovrà tener conto della distanza massima tra sito primario e sito secondario; 3. Progettazione della rete secondaria per l'instradamento alternativo (satellitare, ponte radio, Wimax, Wi-Fi, mobile, ecc...) e dei relativi aspetti di sicurezza; 4.Progettazione della soluzione di gestione e delle relative funzionalità in grado di garantire la gestione centralizzata della rete di DR; 5.Progettazione degli interventi di adeguamento degli ambienti che dovranno ospitare gli apparati e dei relativi aspetti di sicurezza; 6.Cronoprogramma delle attività da concordare tra committente e fornitore. • *Low Level Design* (Progetto di Dettaglio), che prevede le seguenti attività e deliverable: Rete Primaria o Sopralluoghi dei siti cliente (anche sotto il profilo della sicurezza) o Progetto esecutivo (link design) Apparati o Sopralluoghi dei siti cliente (anche sotto il profilo della sicurezza) o Progetto esecutivo (link budget) o Progetto di adeguamento siti Rete secondaria per l'instradamento alternativo o Sopralluoghi o Progetto esecutivo (link budget) o Progetto di adeguamento siti Definizione delle modalità operative per le procedure di gestione o Analisi requisiti o Pianificazione e progettazione processi

	Gestione della soluzione di rete del DR o Definizione delle funzionalità e dei requisiti tecnici o Progetto esecutivo 9. Collaudo o Piano di collaudo 10. Piano complessivo di progetto 11. Metodologia di Project Management
ADEMPIMENTI NON PREVISTI	• Attività operative di PM, procurement materiali, adeguamento siti, installazione, posa in opera, collaudo e formazione • Attività riguardanti l'ottenimento dei permessi necessari alle attività di scavo e/o al rilascio delle frequenze
INDICATORI MINIMI DI SERVIZIO	• Completezza • Rispetto dei Tempi pianificati Accuratezza nella redazione della documentazione prevista
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	• Report periodico sullo Stato Avanzamento Lavori (SAL). • Governance e reporting dei lavori, rispetto del piano di attività • Documentazione attestanti la conformità ai requisiti e titoli autorizzativi • Possesso delle competenze professionali richieste (vedi sotto)
COMPETENZE RICHIESTE	• Competenze sulle principali norme e standard riferiti alle TLC, al DR ed alla sicurezza • Competenze sulle norme per l'attrezzaggio e la gestione di siti per le telecomunicazioni • Competenze tecnologiche previste per le varie soluzioni di rete per il DR
TEMPI DI REALIZZAZIONE	Piccola Amministrazione o Effort : 60-90 gg/u professionali o Elapsed : 1-2 mesi solari Media Amministrazione o Effort : 90-150 gg/u professionali o Elapsed : 2-3 mesi solari Grande Amministrazione o Effort : 150-210 gg/u professionali o Elapsed : 3-4 mesi solari Grandissima Amministrazione o Effort : 210-240 gg/u professionali o Elapsed : 5-6 mesi solari

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Valutabile in numero di giornate/uomo professionali per tariffa professionale di tipo Senior.
COSTI PERIODICI	NA
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	A consumo in funzione dei profili professionali richiesti e del maggior effort per eventuali extracosti necessari al reperimento di eventuali dati necessari alla progettazione. Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA

Sotto-servizio B: Fornitura, manutenzione e gestione, anche in modalità condivisa tra più amministrazioni, dei componenti di rete della soluzione di DR, inclusi quelli necessari alla gestione dell'instradamento alternativo degli accessi dalla periferia in caso di emergenza

PRE-REQUISITI	D1: Consulenza per autovalutazione e predisposizione della documentazione per l'acquisizione del parere ai sensi del comma 4 dell'art. 50 bis del CAD D2 – Servizio di predisposizione dei piani di CO/DR e progettazione organizzativa e tecnologica della soluzione di DR D5 - Servizi di rete e di copia per il DR: Sottoservizio A (Progettazione della soluzione di rete) D3 - Sito di Disaster Recovery: aree CED e aree Posti di Lavoro D4 - Componenti HW e SW della soluzione di DR
CARATTERISTICHE TECNICHE	**Tier 1 e 2**: Non è previsto alcun collegamento di rete tra sito di DR e sito primario; Possono essere previsti collegamenti non ridondati, tra sito di DR ed utenza periferica (interna ed esterna); **Tier 3**: E' previsto un collegamento di rete, anche non ridondato, tra sito di DR e sito primario; Sono previsti collegamenti, anche non ridondati, tra sito di DR ed utenza periferica (interna ed esterna); **Tier 4**: E' previsto un collegamento di rete ridondato tra sito di DR e sito primario; Sono previsti collegamenti di rete ridondati tra sito di DR ed utenza periferica (interna ed esterna); **Tier 5 e 6**: E' previsto un collegamento di rete ridondato e per l'instradamento alternativo tra sito di DR e sito primario; Sono previsti collegamenti di rete ridondati e per l'instradamento alternativo tra sito di DR ed utenza periferica(interna ed esterna);
ADEMPIMENTI PREVISTI	Fatta salva la preventiva verifica circa la disponibilità di eventuali convenzioni/accordi quadro per la PA (es.SPC), il sotto-servizio B, a seconda dei vari tier, prevederà in parte o tutte le seguenti attività: Rete Primaria • Sopralluoghi • Gestione amministrativa dei permessi • Procurement fibra o altra tipologia di connettività (rame, satellitare, ponte radio, ecc...) • Installazione e posa in opera (opere civili e collaudo) Apparati • Sopralluoghi • Predisposizione siti • Procurement apparati TLC, stazioni di energia e sistemi di gestione • Collaudo in fabbrica • Installazione e messa in opera centro di gestione (configurazione e collaudo) • Installazione e messa in opera apparati (configurazione, presa in carico dal centro di gestione e collaudo) Rete secondaria per l'instradamento alternativo • Sopralluoghi • Predisposizione siti • Procurement apparati per l'instradamento alternativo (satellitare, ponte radio, mobile, ecc...), stazioni di energia e centro di gestione • Collaudo in fabbrica • Installazione e messa in opera centro di gestione (configurazione e collaudo) • Installazione e messa in opera apparati (configurazione, presa in carico dal centro di gestione e collaudo) 7. Collaudo di sistema

	8. Manutenzione delle componenti di rete • Help Desk • Correttiva • Preventiva 9. Gestione delle componenti di rete • Presidio I sistemi di gestione delle varie tipologie di apparati, da prevedersi in modalità ridondata (sito primario e sito di DR), dovranno permettere l'effettuazione di attività di pianificazione, installazione, gestione, manutenzione e fornitura di reti e servizi di telecomunicazioni e dovranno essere funzionalmente strutturati secondo il modello a livelli presentato nella raccomandazione ITU-T di riferimento. I sistemi di gestione, infine, dovranno essere in grado di fornire funzionalità di provisioning di link e di circuito end-to-end e allarmistica integrata, attraverso un' integrazione con un livello di Network Management superiore basata su interfaccia standard (ad es. Solution Set for the Multi-Technology Network Management NML-EML Interface), che dovrà risiedere in un apposito centro servizi TLC o NOC (Network Operating Center) eventualmente da prevedersi in modalità "service" (nel caso di piccole e medie amministrazioni) o dedicata (nel caso di aggregati di piccole/medie amministrazioni, di grandi e di grandissime amministrazioni). Il NOC ha l'obiettivo di garantire la gestione integrata di tutti i sistemi di TLC dell'Amministrazione oggetto di fornitura per erogare almeno i seguenti servizi: • Fault Management • Configuration Management • Performance Management • Administration Management • Security Management Il sottoservizio prevede anche la fornitura di personale, eventualmente presso il cliente, specializzato in ambito TLC e DR al fine di supportarlo nelle attività di: • Supervisione, monitoraggio e gestione della soluzione di rete del DR • Condivisione con il cliente della procedura operativa, in caso di scenario di crisi, delle attività a carico del fornitore e l'output desiderato • Collaudi periodici con relativa certificazione fornitore ed utente (relativo alla soluzione di rete) • Gestione del trattamento dei dati personali da parte degli amministratori di sistema, e nel rispetto del DLGS 196/03 all.B, direttiva 95/46/CE del 24/5/12 s.m.i. e successivi provvedimenti del Garante della Privacy, incluse le raccomandazioni e provvedimenti sull'uso delle soluzioni "cloud")
ADEMPIMENTI NON PREVISTI	Supporto al cliente per le problematiche di tipo applicativo durante lo scenario di crisi.
INDICATORI MINIMI DI SERVIZIO	• RPO e RTO compatibili con la tipologia di soluzione scelta • % di alcuni parametri nell'arco della durata del contratto (disponibilità collegamenti, tasso di errore, tempo di latenza, jitter, ecc...) • Tempi di ripristino delle anomalie che impattano sull'erogazione del servizio, sia in caso di scenario "standard" sia in caso di scenario di "crisi" (possono essere concordati anche 2 SLA differenti) • Tempo entro il quale avviene la commutazione tra il centro primario ed il centro di DR e/o tempo entro il quale la periferia è in grado di attestarsi sul centro di DR
STRUMENTI DI VERIFI-CA DELLA CONFOR-MITA' DEL SERVIZIO	• Produzione di certificazioni • Relazioni a seguito di operazioni di test e collaudo • Report sugli SLA
COMPETENZE RICHIESTE	• Competenze sulle principali norme e standard riferiti alle TLC ed al DR • Competenze sulle norme per l'attrezzaggio e la gestione di siti per le telecomunicazioni • Competenze tecnologiche previste per le varie tipologie di soluzioni di rete per il DR

TEMPI DI REALIZZAZIONE (ELAPSED)	• Piccola Amministrazione: 2-4 mesi solari • Media Amministrazione: 4-6 mesi solari • Grande Amministrazione: 6-8 mesi solari • Grandissima Amministrazione: 8-12 mesi solari

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Costi correlati agli investimenti per la realizzazione iniziale della soluzione in base ai requirements del cliente Eventualmente costi di gestione della soluzione per il primo anno (o porzione di anno in cui si avvia il progetto)
COSTI PERIODICI	Canoni di mantenimento e di gestione della soluzione (HW e SW nel caso in cui l'Amministrazione non li acquisti), manutenzioni HW, manutenzioni SW ed altri eventuali servizi). Costi di gestione del contratto (fiscale, legale) Costi di ammortamento delle infrastrutture
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Costi di investimento per l'adeguamento dell'impianto iniziale a seguito di variazioni nei requirements del cliente: aumento e/o variazione dei sistemi di produzione, variazioni degli SLA richiesti dal cliente Adeguamento dei canoni di mantenimento e gestione della soluzione a seguito di variazioni nei requirements del cliente Eventuali costi derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

SCHEDA SERVIZIO:D8

PARTE GENERALE

DENOMINAZIONE	D8 – Servizi di verifica per le soluzioni di DR (audit)
DESCRIZIONE	Incarichi di verifica (audit) condotti da Terza Parte Indipendente sulle diverse componenti del DR/CO; Essi possono includere l'esecuzione di uno o più dei seguenti sotto-servizi: A.verifica dei piani di DR e CO i. con simulazione del disastro ii. senza simulazione del disastro B.verifica delle infrastrutture di DR C.verifica dei test (di simulazione del disastro) D. verifica di conformità dei processi in atto presso l'organizzazione con quelli previsti dagli standard per il DR (ad es. ISO 22301) a fini di gap analysis o di certificazione
CORRISPONDENZA ITIL	Continual Service Improvement
CORRISPONDENZA CPV	72150000-1 Servizi di consulenza per verifiche di sistemi informatici e servizi di consulenza per attrezzature informatiche; 72800000-8 Servizi di audit e collaudo informatico; 72810000-1 Servizi di audit informatico; 72820000-4 Servizi di collaudo informatico;
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT di DigitPA	COP Continuità Operativa; CON Consulenza; PGE Gestione e processi organizzativi; PAQ Assicurazione della Qualità
TIER	1-6

PARTE TECNICA

<u>SOTTO-SERVIZIO A:</u>
VERIFICA (audit) dei piani di DR e CO,
i. con simulazione
oppure
ii. senza simulazione del disastro

PRE-REQUISITI	• Implementazione totale o parziale di un processo di Continuità Operativa e/o Disaster Recovery • Definizione di una strategia di test del piano di Continuità Operativa e Disaster Recovery oppure requisiti/vincoli di riferimento a cui ispirare detta strategia • Presenza totale o parziale dei Piani di definizione degli scenari di crisi, di gestione degli incidenti, di invocazione delle procedure di recovery, di comunicazione, di rientro alla normalità • Presenza della documentazione che descrive il piano di Continuità Operativa. • Presenza della documentazione di Autovalutazione e dello Studio di Fattibilità Tecnica • In caso di servizio in outsourcing, la possibilità - contrattualmente prevista di i. effettuare l'attività di simulazione *oppure* ii. effettuare l'attività di auditing coinvolgendo l'outsourcer
CARATTERISTICHE TECNICHE	Il servizio di audit ha lo scopo di: - verificare l'adeguatezza, la coerenza e la pertinenza dei piani rispetto all'organizzazione dell'Ente ed al contesto di riferimento

	- verificare l'applicabilità e/o l'applicazione delle strategie o dei requisiti/vincoli indicati dall'Ente per il test dei piani di Continuità Operativa e/o Disaster Recovery; - verificare il funzionamento delle procedure e delle soluzioni tecniche e tecnologiche necessarie per reagire alla situazione di disastro che l'Ente intende simulare ed il rispetto dei Recovery Time Objective definiti; - verificare i processi descritti nel piano di CO al fine di valutare l'adeguatezza e la coerenza delle soluzioni adottate, rispetto ai requisiti di business dell'Ente - verificare la gestione delle modifiche ai piani - identificate le eventuali azioni di rimedio alle eccezioni/punti di miglioramento evidenziati dai test.
ADEMPIMENTI PREVISTI	Nel caso in cui l'audit venga svolto **con simulazione del disastro**, il fornitore avrà il compito di: • definire un piano di test, identificando i diversi scenari di test che potranno essere simulati (table-top testing, emergency communication testing, datacenter recovery testing, work-area testing), nell'ambito della strategia pre-definita dall'Ente. • determinare la tempistica di esecuzione dei test • descrivere gli obiettivi chiave di ogni test • definire i ruoli e le responsabilità delle persone coinvolte nelle attività di test per una corretta pianificazione ed esecuzione • predisporre la documentazione con formati standard a supporto della pianificazione, esecuzione, reporting, consuntivazione dei test, modalità di comunicazione all'interno dell'azienda e con terze parti • condurre i test secondo il piano stabilito assicurando lo svolgimento delle seguenti fasi: ✓ Pre-test - E' l'insieme di azioni necessarie per preparare l'ambiente per la simulazione vera e propria inclusi l'illustrazione / attivazione dello scenario di test oggetto della simulazione, la comunicazione alle diverse funzioni aziendali e/o terze parti dello scenario di test. ✓ Test - E' la vera e propria attivazione delle procedure di recovery. Si eseguono le attività operative vere e proprie gli obiettivi specifici del piano di BCM e/o DRP quali ad esempio l'attività di immissione dati, telefonate, elaborazione dati, trattamento di ordini, e movimenti di personale, apparecchiature e fornitori. ✓ Post-test - chiusura delle attività dei gruppi. Questa fase comprende compiti quali riportare tutte le risorse al posto opportuno, sconnettere le apparecchiature e rimandare indietro il personale, cancellare tutti i dati dell'azienda dai sistemi ospitanti, come pure valutare formalmente il piano ed apportare i miglioramenti indicati. • Durante la conduzione dei test il fornitore dovrà supportare l'Ente svolgendo un ruolo di facilitatore e conduttore dello scenario di test, illustrando alle diverse parti coinvolte gli scenari di test ed eventuali evoluzioni che possano interessare questi ultimi; • Rilevare e valutare l'esito dei test condotti ed interpretarne i relativi risultati • Individuare, descrivere e comunicare le eventuali azioni di rimedio necessarie, attribuendo i diversi livelli di criticità, e suggerire le relative verifiche di follow-up Inoltre: • la prova dovrebbe essere programmata per un periodo che comporti il minimo disturbo alle normali operazioni (i fine settimana rappresentano normalmente un ottimo periodo per effettuare le prove); • è importante che il personale chiave dei vari team di ripristino sia coinvolto nel test del processo e disponga del tempo occorrente per svolgere adeguatamente la propria attività; • la prova dovrebbe riguardare tutti le componenti critiche e simulare le condizioni elaborative dei picchi di lavoro, anche se è eseguito in momenti di inattività • la prova dovrebbe includere componenti che sono state modificate nel corso

	dell'ultimo periodo (*change management* dei piani di CO/DR). Nel caso in cui l'audit sia svolto **senza simulazione del disastro**, il fornitore avrà il compito di: • Verificare e validare i documenti di BIA e RA, ove presenti, e la loro coerenza rispetto alla documentazione dei piani di DR e CO • Verificare la presenza, l'adeguatezza, la coerenza delle strutture necessarie alla DR e CO (risorse tecnologiche e logistiche), rispetto alla documentazione di cui al punto precedente • Verificare la presenza degli scenari di crisi; • Verificare la presenza, l'adeguatezza e la coerenza dei processi di escalation idonei a determinare la dichiarazione dello stato di crisi; • Verificare la presenza, l'adeguatezza e la coerenza delle strutture di governo del Piano di DR; • Verificare la presenza, l'adeguatezza e la coerenza delle strutture tecniche e organizzative necessarie alla valutazione dell'evento disastroso; • Verificare e validare l'adeguatezza e la coerenza dell'organizzazione complessiva necessaria alla gestione degli scenari di crisi individuati ed alla CO (numero di risorse, competenze, skill, ecc.); • Verifica e validazione del piano di gestione della crisi (modello organizzativo e gerarchico) • Verifica del piano e della soluzione di DR; • Verifica della completezza delle informazioni, presenti nel piano di DR relativamente alle comunicazioni interne ed esterne all'Ente, agli owner dei processi, ecc.. • Verifica del rispetto delle normative generali e/o di settore; • Se presenti, verifica dell'adeguatezza e coerenza dei contratti stipulati con fornitori esterni di servizi rispetto a quanto stabilito nel piano di DR e ai valori di RPO e RTO previsti; • Verifica delle procedure di simulazione previste per il test dei piani di DR e CO • Verifica sull'adeguatezza, coerenza e completezza delle procedure operative; • Verifica del corretto piano di manutenzione del piano di DR; • Verifica della presenza, adeguatezza e coerenza dei processi e della documentazione relativa alla gestione operativa del Piano di DR e degli scenari connessi (verbali sull'impatto dell'evento, dichiarazione dell'evento, attivazione fornitori critici, stato di avanzamento del Piano di recovery,etc..) • Verifica della presenza, adeguatezza e coerenza degli strumenti per la gestione del Piano di DR (canali comunicativi, postazioni di lavoro, locali, procedure operative) • Verifiche a campione sui controlli previsti dal Piano di DR • Se presenti, verifica dell'adeguatezza e coerenza dei contratti stipulati con fornitori esterni di servizi rispetto a quanto stabilito nel piano di CO e ai valori di RPO e RTO previsti • Verifica del corretto piano di manutenzione del piano di CO • Verifica dell'esistenza del processo di aggiornamento delle procedure previste nei piani di DR/CO in caso di modifiche intervenute (*change management*) • Identificare, descrivere e comunicare le azioni di rimedio raccomandabili e le relative verifiche di follow-up Le verifiche di adeguatezza e coerenza (senza simulazione del disastro) dovranno essere condotte sulla base di: • elementi di coerenza tra i diversi documenti predisposti dall'Ente e dai fornitori • elementi di coerenza rispetto all'organizzazione ed all'infrastruttura

	informatica in essere presso l'Ente • Best Practice e standard internazionali di riferimento (quali ad esempio ISO22301, ISO/IEC 24762:2008) • Elementi di coerenza rispetto alla strategia dichiarata dall'Ente, ove presente, ed ai requisiti ed ai vincoli impliciti o espressi dall'Ente. • Confronto con analoghe esperienze e prassi in Enti assimilabili, ove disponibili
ADEMPIMENTI NON PREVISTI	Il fornitore non svolgerà azioni di rimedio a fronte delle eventuali eccezioni riscontrate nel corso dell'audit, né le relative verifiche di follow-up. Nell'ambito dello svolgimento del servizio secondo **l'opzione (i)**, **con simulazione del disastro**, l'erogatore del servizio non svolgerà verifiche sul piano di DR/CO per quelle componenti al di fuori del perimetro delle procedure necessarie per reagire alla simulazione della situazione di disastro, come prevista dalla strategia di test identificata dall'Ente. Nell'ambito dello svolgimento del servizio secondo **l'opzione (ii)**, **senza simulazione del disastro,** l'erogatore del servizio non svolgerà simulazioni di situazioni di disastro.
INDICATORI MINIMI DI SERVIZIO	Ogni valutazione di *professional judgment* (giudizio professionale) e *professional skepticism* (scetticismo professionale), applicati dall'auditor, sia nello svolgimento delle verifiche e nell'interpretazione dei risultati delle verifiche svolte, dovrà essere motivata ed argomentata per iscritto. **Verifiche con simulazione del disastro (i)** Il test di simulazione del disastro devono essere condotti coerentemente con la strategia di test e/o i requisiti/vincoli indicati dall'Ente. I test di simulazione del disastro devono essere in grado di: • verificare la completezza e precisione delle informazioni contenute nel piano d'emergenza, • valutare le prestazioni del personale coinvolto nell'esercitazione, • stimare il livello di addestramento e di consapevolezza dei membri di gruppi non collegati con l'emergenza, • valutare il coordinamento tra il gruppo d'emergenza e fornitori terzi, • misurare l'adeguatezza, la coerenza e la capacità del sito sostitutivo ad effettuare le elaborazioni prescritte, • valutare la capacità di accedere ad informazioni registrate essenziali, • valutare lo stato e quantità di apparecchiature e attrezzature poste presso il sito di recovery, • misurare le prestazioni complessive delle attività operative e di elaborazione dati, relative al mantenimento della continuità aziendale. **Verifiche senza simulazione del disastro (ii)** Fornitura di documentazione di audit che, per ognuno degli aspetti verificati, riporti il target previsto nel piano di DR e il livello effettivo risultante dall'audit, con evidenza di eventuali carenze tecniche/organizzative/contrattuali e con l'indicazione di possibili ipotesi di soluzione. Con riferimento all'intero piano di CO, il servizio dovrà documentare la valutazione assegnata ai vari elementi presenti. In particolare dovrà valutarne l'adeguatezza, la coerenza, la completezza, la rispondenza ai requisiti dell'Ente ed agli standard per la predisposizione di piani di CO, specificando per ogni elemento ritenuto non più valido le motivazioni e suggerendo le azioni correttive da intraprendere. Il fornitore dovrà integrare la documentazione con questionari, interviste o altro materiale utilizzato in fase di auditing.
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	Controlli intermedi sullo stato di avanzamento delle attività anche attraverso la condivisione della documentazione predisposta, anche in versione "bozza". Tale documentazione dovrà contenere risposte puntuali (sezioni e paragrafi) in riferimento alla lista degli adempimenti previsti. che diano inoltre una

	rappresentazione sotto forma di "cruscotto" di valutazione dell'esito dei test.
COMPETENZE RICHIESTE	• Competenze di IT audit • Competenze metodologiche sugli standard di riferimento in ambito Business Continuity e Disaster Recovery (quali ad esempio ISO22301, ISO/IEC 24762:2008) • Competenze metodologiche sullo standard ITIL di riferimento • Competenze organizzative e di processo in ambito PA • Competenze di mercato del settore di riferimento • Competenze contrattuali in ambito ICT • Competenze relazionali • Competenze di Project Management
TEMPI DI REALIZZAZIONE	Da 2 settimane a 6 mesi (tempi elapsed) dipendentemente da: • complessità organizzativa e tecnologica dell'Ente • presenza nel piano di DR di più livelli di *tier* • livello del *tier* • perimetro definito • fornitori e società/Enti esterni coinvolti • periodi (fasce orarie e giorni) selezionati per la simulazione (ad es. week end) • implementazione della soluzione verificata (in house, in outsourcing, in cloud) • numero dei fornitori coinvolti nella simulazione Indicativamente: Ente piccolo - da 2 a 4 settimane Ente medio - da 3 a 8 settimane Ente grande - da 2 a 4 mesi Ente grandissimo - da 3 a 6 mesi

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Numero di giornate o a corpo in funzione di: - complessità organizzativa e tecnologica dell'Ente - presenza nel piano di DR di più livelli di tier - livello del tier - perimetro definito - fornitori e società/Enti esterni coinvolti - periodi (fasce orarie e giorni) selezionati per la simulazione (ad es. week end) - implementazione della soluzione verificata (in house, in outsourcing, in cloud) - numero dei fornitori coinvolti nella simulazione
COSTI PERIODICI	Non previsti in caso di attività una tantum. Canone annuale se previsto audit periodico o con periodicità stabilita e concordata con l'Ente sulla base di una strategia prestabilita, così come richiesto da tutti gli standard internazionali di riferimento (es. ISO 22301) e dalle linee guida.
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni necessari per l'attività di auditing. Attività fuori dagli ordinari orari d'ufficio (es. notturne o in giorni festivi e pre-festivi). Eventuali attivita derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA

SOTTO-SERVIZIO B:
Servizi di verifica sulle infrastrutture di DR

PRE-REQUISITI	• Implementazione della soluzione di Disaster Recovery • Presenza della documentazione del piano di DR • In caso di outsourcing totale o parziale dei servizi di DR: ✓ disponibilità della documentazione dei contratti di fornitura stipulati dall'ente per l'approvvigionamento dei servizi di DR; ✓ presenza, nei succitati contratti, della possibilità da parte di terzi di effettuare l'auditing sui servizi di DR forniti in outsourcing • Se presente un piano di CO, disponibilità della relativa documentazione.
CARATTERISTICHE TECNICHE	Il servizio ha lo scopo di verificare le soluzioni e le caratteristiche tecniche delle infrastrutture indicate dall'Ente come sito secondario rispetto agli obiettivi specificati nel piano di DR e la sua pertinenza rispetto all'organizzazione ed al contesto di riferimento. Le verifiche devono essere periodiche, così come richiesto da tutti gli standard internazionali di riferimento (es. ISO 22301) e dalle linee guida.
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di verificare/valutare che gli aspetti di seguito elencati risultino adeguati rispetto alla criticità dei servizi e agli obiettivi specificati nel piano di DR e pertinenti rispetto all'organizzazione ed al contesto di riferimento: • Sito secondario di recovery - posizione geografica e alle caratteristiche dell'immobile: ✓ Distanza e raggiungibilità (vicinanza autostrade, strade statali, percorsi alternativi, ecc.); ✓ Caratteristica della zona in relazione ad eventi catastrofici quali frane, inondazioni, alluvioni, ecc.; ✓ Adeguatezza e coerenza e regolarità della struttura permessi/concessioni Comunali; ✓ Valutazione di rischio idro-geologico coerente con la l'area geografica che ospita il sito; • Caratteristiche impianti del Data Center secondario e loro ridondanza.; ✓ Distribuzione elettrica primaria (potenza e locali); ✓ Gruppi di continuità UPS (potenza, autonomia e locali); ✓ Gruppo elettrogeno (potenza, riserva carburante, piano test periodici); ✓ Doppia alimentazione dei singoli rack; ✓ Impianto di rilevazione fumi e calore; ✓ Impianto di spegnimento incendi; ✓ Impianto di rilevazione allagamenti; ✓ Pavimento flottante; ✓ Impianto di condizionamento con sensori per controllo della temperatura ed umidità; ✓ Porte a contenimento del fuoco per la separazione di aree interne o adiacenti il DC; ✓ Sistema di controllo accessi (identificazione e autenticazione); ✓ Sistema di video sorveglianza e di antintrusione all'interno del DC; ✓ Protezione perimetrale dell'edificio; ✓ Vigilanza. • Controllo e gestione remota allarmi, monitoraggio stato impianti; • Caratteristiche infrastruttura IT: ✓ Rete geografica e locale; ✓ Potenza elaborativa (dedicata/condivisa); ✓ Storage (dimensionamento);

	• Locali per postazioni di lavoro per test, collaudo, emergenza: o Attrezzaggio (rete elettrica, dati e fonia); o Mobilio • Caratteristiche tecnico/contrattuali del servizio offerto da terze parti: ✓ Verifica della corrispondenza tra i servizi, acquisiti con contratti di outsourcing, e i relativi Livelli di Servizio rispetto quanto specificato nei piani di DR, con particolare attenzione rispetto agli obiettivi di RTO/RPO e alla criticità dei servizi dell'Ente; ✓ Per il servizio di DR in outsourcing, controllo e verifica, presso fornitore terzo, della corrispondenza dei servizi e delle infrastrutture rispetto ai contratti • Valutare e comunicare gli esiti delle verifiche, suggerendo le azioni di rimedio e le successive verifiche di follow-up Le verifiche di adeguatezza e coerenza dovranno essere condotte anche sulla bas di: • elementi di coerenza tra i diversi documenti predisposti dall'Ente e dai fornitori • elementi di coerenza rispetto all'organizzazione ed all'infrastruttura informatica in essere presso l'Ente • Best Practice e standard internazionali di riferimento (quali ad esempio ISO22301, ISO/IEC 24762:2008) • Elementi di coerenza rispetto alla strategia dichiarata dall'Ente, ove presente, ed ai requisiti/vincoli impliciti o espressi dall'Ente • Confronto con analoghe esperienze e prassi in Enti assimilabili, ove disponibili
ADEMPIMENTI NON PREVISTI	Il fornitore del servizio non svolgerà test operativi, né simulazioni di disastro relativamente alle infrastrutture di DR. Non verrà svolto un audit delle caratteristiche dell'intero piano di DR/CO, ma la sua coerenza di alcune sue componenti infrastrutturali rispetto al contesto di riferimento. Inoltre, non saranno incluse le azioni di rimedio a fronte delle eventuali eccezioni riscontrate, né le relative verifiche di follow-up.
INDICATORI MINIMI DI SERVIZIO	Fornitura di documentazione di audit che, per ognuno degli aspetti previsti, riporti il target previsto nel piano di DR e il livello effettivo risultante dall'audit, con evidenza di eventuali carenze realizzative/contrattuali e con l'indicazione di possibili ipotesi di soluzione. Verbale della visita ispettiva (ove prevista) presso il fornitore terzo dei servizi di DR. Ogni valutazione di *professional judgment* (giudizio professionale) e *professional skepticism* (scetticismo professionale), applicati dall'auditor, sia nello svolgimento delle verifiche che nell'interpretazione dei risultati delle verifiche svolte, dovrà essere motivata ed argomentata per iscritto.
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	Controlli intermedi sullo stato di avanzamento delle attività anche attraverso la condivisione della documentazione predisposta, anche in versione "bozza". Tale documentazione dovrà contenere risposte puntuali (sezioni e paragrafi) in riferimento alla lista degli adempimenti previsti.
COMPETENZE RICHIESTE	• Competenze di IT audit • Competenze metodologiche sugli standard di riferimento in ambito Business Continuity e Disaster Recovery (quali ad esempio ISO22301, ISO/IEC 24762:2008) • Competenze di organizzative e di processo in ambito PA • Competenze di mercato del settore di riferimento • Competenze contrattuali in ambito ICT • Competenze relazionali

	• Competenze di Project Management • Competenze sistemistiche, architetturali, di rete e di database
TEMPI DI REALIZZAZIONE	Indicativamente da 1 a 3 mesi (tempo *elapsed*) in base a: • Livello del *tier* • Complessità organizzative e tecnologiche dell'Ente • Scelta di implementazione della soluzione di DR (in house, in outsourcing, cloud) • Numero dei fornitori coinvolti nella soluzione di DR

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Numero di giornate o a corpo in funzione di: - Livello del *tier* - Complessità della soluzione tecnica adottata - Complessità organizzative e tecnologiche dell'Ente - Scelta di implementazione della soluzione di DR (in house, in outsourcing, cloud) - Numero dei fornitori coinvolti nella soluzione di DR I tempi elapsed possono essere stimati **indicativamente** come segue: • Ente piccolo: da 1 a 4 settimane • Ente medio: da 2 a 6 settimane • Ente grande: da 1 a 2 mesi • Ente grandissimo: da 2 a 3 mesi
COSTI PERIODICI	Non previsti in caso di attività Una Tantum. Canone annuale se previsto come audit periodico all'interno di contratto pluriennale, così come richiesto da tutti gli standard internazionali di riferimento (es. ISO 22301) e dalle linee guida.
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni, necessari per l'attività di auditing. Attività fuori dagli ordinari orari d'ufficio (es. notturne o in giorni festivi e pre-festivi). Eventuali attività derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA

SOTTO-SERVIZIO C:
Audit sui test di simulazione del disastro

PRE-REQUISITI	• Implementazione totale o parziale di un processo di Continuità Operativa e/o Disaster Recovery • Definizione ed attuazione di una strategia e di un piano di test di simulazione delle procedure di Disaster Recovery e Continuità Operativa • In caso di test presso l'outsourcer, la possibilità - contrattualmente prevista – di effettuare l'attività di auditing dei test
CARATTERISTICHE TECNICHE	Il servizio di audit ha lo scopo di verificare: - la periodicità delle verifiche e dei test di simulazione - l'applicazione delle strategie definite dall'Ente per il test dei piani di Continuità Operativa e/o Disaster Recovery; - l'esito delle verifiche condotte, incluse le azioni identificate per rimediare alle eccezioni/punti di miglioramento evidenziati dai test. L'audit deve essere periodico, così come richiesto da tutti gli standard internazionali di riferimento (es. ISO 22301) e dalle linee guida.
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di: 1. Rilevare e verificare la strategia e la periodicità di test definita e nello specifico: • Le tipologie e modalità di test che sono state identificate: analisi critica delle procedure, simulazione a tavolino, simulazione nella realtà; • La frequenza con cui devono essere condotti i test e le modalità di identificazione del perimetro di processi/ applicativi da verificare; • Modalità di definizione e documentazione degli scenari di riferimento per i test; • Coerenza tra gli scenari di test identificati e le strategie di recovery definite nei piani di CO e DR • La presenza di un piano formale di test eventualmente pluriennale 2. Rilevare e verificare le modalità di conduzione dei test e nello specifico: • Le attività di test condotte nel corso del periodo di riferimento oggetto dell'audit; • La coerenza delle attività di test condotte rispetto al piano definito • La partecipazione di un gruppo significativo di utenti alle attività di test anche in funzione del loro coinvolgimento (CO Champion, Risorse critiche) e del dipartimento/funzione di appartenenza (Processi di business, IT, ecc…) • La definizione di chiari obiettivi di test che dovranno essere valutati nel corso delle verifiche e Recovery Time Objective che dovranno essere rispettati 3. Rilevare e verificare la documentazione a supporto dei test e nello specifico • Elenco delle persone che hanno partecipato alle attività di test • Evidenze di audit delle attività condotte nella simulazione e delle tempistiche per lo svolgimento delle attività • Verbali e memo a supporto delle attività di debriefing finale • Evidenza di eccezioni o eventi non previsti identificati nel corso dei test • Risultati delle attività di test ed indicazione delle azioni di miglioramento/integrazione dei piani di CO e DR 4. Rilevare e valutare l'esito dei test condotti ed interpretarne i relativi risultati in termini di: • esito ottimale: nessuna debolezza o eccezione individuata nel corso dello svolgimento del test: • Esito soddisfacente: nessuna eccezione rilevata, con l'identificazione di aree di miglioramento • Esito critico/molto critico in caso di eccezioni più o meno significative. 5. Comunicare gli esiti delle verifiche, suggerendo le azioni di rimedio e le

	verifiche di follow-up successivi.
ADEMPIMENTI NON PREVISTI	L'erogatore del servizio non svolgerà verifiche sui test delle procedure di DR/CO per quelle componenti al di fuori del perimetro delle procedure necessarie per reagire alla simulazione della situazione di disastro. Inoltre, non saranno incluse le azioni di rimedio a fronte delle eventuali eccezioni riscontrate, né le relative verifiche di follow-up.
INDICATORI MINIMI DI SERVIZIO	Il servizio dovrà documentare la valutazione assegnata alle modalità di svolgimento dei test ed ai relativi esiti. In particolare dovrà valutare • la completezza, l'adeguatezza e coerenza , la rispondenza della strategia di test rispetto agli standard di riferimento per la predisposizione di piani di verifica di CO e DR, • l'adeguatezza e coerenza delle modalità di conduzione dei test • la documentazione dei test • la valutazione degli esiti dei test, specificando per ogni elemento ritenuto non più valido le motivazioni e suggerendo le azioni correttive da intraprendere. Il fornitore dovrà integrare la documentazione con questionari, interviste o altro materiale utilizzato in fase di auditing. Ogni valutazione di *professional judgment* (giudizio professionale) e *professional skepticism* (scetticismo professionale), applicati dall'auditor, sia nello svolgimento delle verifiche che nell'interpretazione dei risultati delle verifiche svolte, dovrà essere motivata ed argomentata per iscritto.
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	Controlli intermedi sullo stato di avanzamento delle attività anche attraverso la condivisione della documentazione predisposta, anche in versione "bozza". Tale documentazione dovrà contenere risposte puntuali (sezioni e paragrafi) in riferimento alla lista degli adempimenti previsti.
COMPETENZE RICHIESTE	• Competenze di IT audit • Competenze metodologiche sullo standard ITIL di riferimento • Competenze metodologiche sugli standard di riferimento in ambito Business Continuity e Disaster Recovery (quali ad esempio ISO22301, ISO/IEC 24762:2008) • Competenze organizzative e di processo in ambito PA • Competenze di mercato del settore di riferimento • Competenze contrattuali in ambito ICT • Competenze relazionali • Competenze di Project Management
TEMPI DI REALIZZAZIONE	Indicativamente da 1 settimana a 6 mesi (tempi elapsed) dipendentemente da: • complessità organizzativa e tecnologica dell'Ente • livello del tier • perimetro definito • fornitori e società/Enti esterni coinvolti • periodi (fasce orarie e giorni) selezionati per la simulazione (ad es. week end) • implementazione della soluzione verificata (in house, in outsourcing, in cloud) • numero dei fornitori coinvolti nella simulazione I tempi elapsed possono essere stimati come segue: • Ente piccolo: da 1 a 4 settimane • Ente medio: da 2 a 8 settimane • Ente grande: da 2 a 4 mesi • Ente grandissimo: da 3 a 6 mesi

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Numero di giornate o a corpo in funzione della complessità organizzativa e tecnologica dell'Ente: livello del *tier,* perimetro definito, fornitori e società/Enti esterni coinvolti, periodi (fasce orarie e giorni) selezionati per la simulazione (ad es. week end), - implementazione della soluzione verificata (in house, in outsourcing, in cloud), - numero dei fornitori coinvolti nella simulazione.
COSTI PERIODICI	Attività periodica, con la medesima periodicità prevista dal piano di test di DR/CO, così come richiesto da tutti gli standard internazionali di riferimento (es. ISO 22301) e dalle linee guida.
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni, necessari per l'attività di auditing. Attività fuori dagli ordinari orari d'ufficio (es. notturne o in giorni festivi e pre-festivi). Eventuali attività derivanti da variazioni in corso d'opera da concordare con l'Amm.ne/Ente committente e da valorizzare con lo stesso parametro utilizzato per la stima dei tempi e costi di realizzazione/erogazione del servizio

PARTE TECNICA

SOTTO-SERVIZIO D:

verifica di conformità dei processi in atto presso l'organizzazione con quelli previsti dagli standard per il DR (ad es. ISO 22301) a fini di gap analysis o di certificazione

PRE-REQUISITI	• Implementazione totale o parziale di un processo di Continuità Operativa e/o Disaster Recovery • In caso di test presso l'outsourcer, la possibilità - contrattualmente prevista – di effettuare attività di verifica
CARATTERISTICHE TECNICHE	Il servizio di audit ha lo scopo di verificare quanto l'organizzazione ed i processi dell'Ente si discostano o risultano conformi rispetto agli adempimenti ed processi previsti dallo standard prescelto, finalizzati alla certificazione del Sistema di Gestione della Continuità Operativa
ADEMPIMENTI PREVISTI	Il fornitore avrà il compito di: 1. Rilevare la conformità o gli eventuali scostamenti rispetto allo standard di riferimento selezionato 2. Rilevare e valutare l'esito dei test condotti ed interpretarne i relativi risultati in termini di: • esito ottimale: nessuna debolezza o eccezione individuata nel corso dello svolgimento dell'analisi • Esito soddisfacente: nessuna eccezione rilevata, con l'identificazione di aree di miglioramento • Esito critico/molto critico in caso di eccezioni più o meno significative. 3. Comunicare gli esiti delle verifiche, suggerendo le azioni di rimedio per colmare i gap , nel caso di gap analisys o l'esito della verifica ai fini della certificazione
ADEMPIMENTI NON PREVISTI	Analisi di aspetti non confrontabili con lo standard di riferimento prescelto. Implementazione delle azioni di rimedio suggerite
INDICATORI MINIMI DI SERVIZIO	Il servizio dovrà documentare la valutazione assegnata rispetto ai gap individuati Ogni valutazione di *professional judgment* (giudizio professionale) e *professional skepticism* (scetticismo professionale), applicati dall'auditor, sia nello svolgimento delle verifiche che nell'interpretazione dei risultati delle verifiche svolte, dovrà essere motivata ed argomentata per iscritto.
STRUMENTI DI VERIFICA DELLA CONFORMITA' DEL SERVIZIO	Controlli intermedi sullo stato di avanzamento delle attività anche attraverso la condivisione della documentazione predisposta, anche in versione "bozza". Tale documentazione dovrà contenere risposte puntuali (sezioni e paragrafi) in riferimento alla lista degli adempimenti previsti.
COMPETENZE RICHIESTE	Competenze metodologiche sugli standard di riferimento in ambito Business Continuity e Disaster Recovery (quali ad esempio ISO22301, ISO/IEC 24762:2008)

	In caso di richiesta di un sottoservizio di certificazione, tale servizio deve essere prestato un Ente di certificazione accreditato per lo specifico standard
TEMPI DI REALIZZAZIONE	Indicativamente da 1 settimana a 6 mesi (tempi elapsed) dipendentemente da:complessità organizzativa e tecnologica dell'Ente, livello del tier, perimetro definito, fornitori e società/Enti esterni coinvolti, implementazione della soluzione verificata (in house, in outsourcing, in cloud). I tempi elapsed possono essere stimati come segue: • Ente piccolo: da 1 a 4 settimane • Ente medio: da 2 a 8 settimane • Ente grande: da 2 a 4 mesi • Ente grandissimo: da 3 a 6 mesi

PARTE ECONOMICA (Componenti di costo)

COSTI UNA TANTUM	Numero di giornate o a corpo in funzione della complessità organizzativa e tecnologica dell'Ente
COSTI PERIODICI	Se prevista una verifica periodica o analisi di follow-up a seguito delle azioni di rimedio
COSTI DI EVENTUALI ATTIVITA' AGGIUNTIVE	Trasferte per interventi presso le sedi dell'Ente, presso il Sito secondario e presso eventuali fornitori esterni, necessari per l'attività di auditing.

2012