SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

LA NORMATIVA

La Continuità Operativa: un obbligo per tutti i Comuni

Il Codice dell'Amministrazione Digitale (Decreto legislativo 7 marzo 2005, n. 82, alla luce del decreto-legge 22 giugno 2012 n. 83 e 6 luglio 2012 n 95 convertiti con modificazioni, rispettivamente, dalla L. 7 agosto 2012, n. 134 e L. 7 agosto 2012, n. 135 e del decreto-legge 4 ottobre 2012 sull'Agenda digitale) all'art. 50-bis rubricato "Continuità operativa" impone alle Pubbliche Amministrazioni, centrali e locali, di predisporre i Piani di Disaster Recovery e di Business Continuity a salvaguardia dei servizi erogati a cittadini e imprese.

Le "Linee guida per il disaster recovery delle pubbliche amministrazioni ai sensi del comma 3, lettera b) dell'art. 50-bis del DLgs. n. 82/2005 e s.m.i." pubblicate il 26/06/2011 da DigitPA (ora "Agenzia per l'Italia Digitale"), sentito il Garante per la protezione dei dati personali, dettagliano gli strumenti per ottemperare agli obblighi derivanti dall'art. 50-bis del CAD, a partire da un percorso di autovalutazione, dalla metodologia per l'individuazione dei rischi (Business Impact Analist BIA) al fine di produrre uno Studio di Fattibilità Tecnica per il Piano di Continuità Operativa e il Piano di Disaster Recovery, da presentare al DigitPA stesso per poi implementare le soluzioni previste nei piani anche sulla base dei pareri espressi dallo stesso DigitPA.

La Circolare del Ministero dell'Interno n. 26 del 28-10-2011 nell'ipotesi di blocco del sistema informatico comunale ricorda che le pubbliche amministrazioni sono tenute ad adottare le misure previste dall'art. 50 bis sopra citato.

La Circolare DigitPA 1 dicembre 2011, n. 58 (G.U. 27.12.2011 n. 300) fornisce le indicazioni necessarie ad adempiere a quanto previsto dal citato articolo 50-bis del CAD e, in particolare, riporta le informazioni che le amministrazioni devono inviare a DigitPA, ai fini del rilascio del Parere sugli Studi di Fattibilità Tecnica (SFT) come previsto dal comma 4, nonché le informazioni che le amministrazioni devono inviare ai fini dell'attività di verifica del costante aggiornamento dei Piani di Disaster Recovery (DR), previste dal comma 3, lettera b) anche al fine di predisporre una informativa annuale per il Ministro per la Pubblica Amministrazione e l'Innovazione.

Gli adempimenti dei Comuni per l'attuazione dell'art.50–bis "continuità operativa" del CAD

La prima parte della Circolare n. 58/2011 riporta le informazioni che le Amministrazioni devono inviare all'Agenzia per l'Italia Digitale ai fini del rilascio del parere sugli Studi di Fattibilità Tecnica (SFT) e le modalità di presentazione delle richieste come previsto dal comma 4, art. 50 bis del CAD. La seconda parte della Circolare riporta le informazioni che le Amministrazioni devono inviare all'Agenzia per l'Italia Digitale ai fini dell'attività di verifica del costante aggiornamento dei Piani di Disaster Recovery (DR), previste dal comma 3, lettera b), art. 50 bis, del CAD.

Lo Studio di Fattibilità Tecnica (SFT) deve essere compilato dalla singola Amministrazione comunale e inviato da parte del "Responsabile della Continuità Operativa" all'Agenzia per l'Italia Digitale.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Nel caso di una Amministrazione articolata in diverse strutture che operano in modo autonomo, lo SFT dovrà essere comunque unico (cfr. capitoli 5 e 7 delle linee guida e relative appendici).

La richiesta di parere sullo SFT, predisposta in ottemperanza all'art. 50 bis del CAD, deve essere trasmessa mediante posta elettronica certificata (PEC) dal Responsabile della Continuità Operativa dalla casella PEC dell'Amministrazione.

La richiesta di parere sullo SFT, deve essere inoltrata sia dai Comuni che non dispongono di Piani e soluzioni di Continuità Operativa / Disaster Recovery sia dai Comuni che già si sono dotate degli stessi. Il messaggio di PEC deve avere in allegato:

- la richiesta di parere sullo SFT;
- la relazione su gli obiettivi complessivi che il Comune si propone di raggiungere ai fini della digitalizzazione e dell'attuazione degli adempimenti del CAD, nonché per assicurare il rispetto delle Regole Tecniche previste dal CAD;
- lo SFT in formato elettronico liberamente rielaborabile e uno o più file contenenti gli esiti della autovalutazione eseguita mediante lo strumento di autovalutazione descritto nelle Linee Guida;
- i riferimenti del "Responsabile della Continuità Operativa", per eventuali richieste di informazioni e chiarimenti.

Per l'emissione del parere, l'Agenzia per l'Italia Digitale prende in considerazione elementi di natura sia tecnica che strategica.

Il **Piano di Disaster Recovery (PDR)** va definito dalle Amministrazioni comunali, una volta ricevuto il parere di Agenzia per l'Italia Digitale e va inviato, in formato elettronico, sempre dalla casella PEC dell'Amministrazione.

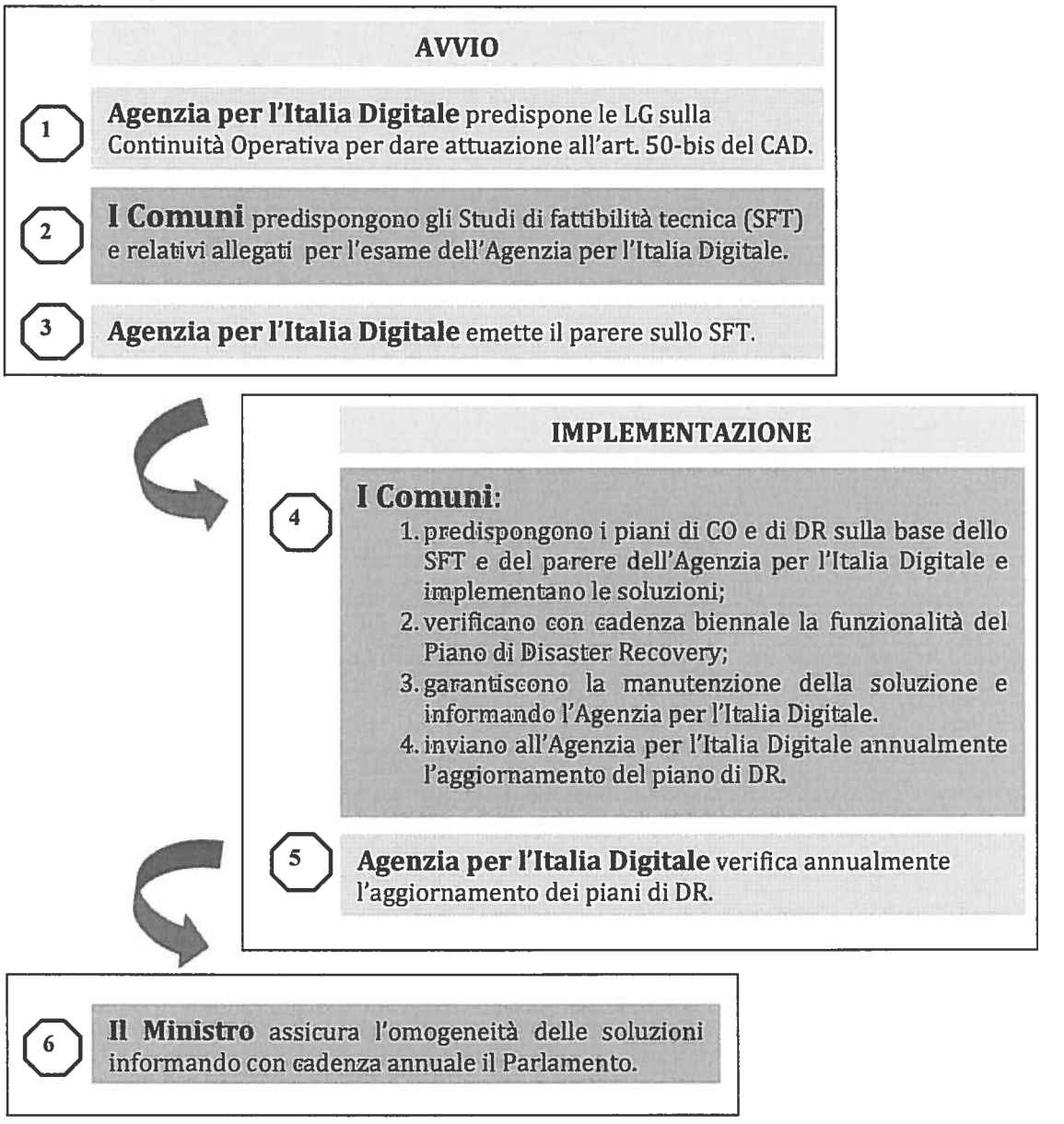
Con cadenza annuale, entro il 31 dicembre di ogni anno, le Amministrazioni devono inviare all'Agenzia per l'Italia Digitale, da parte del Responsabile della Continuità Operativa dalla casella PEC del Comune, la versione aggiornata del Piano di DR in formato elettronico unitamente alla dichiarazione che, in relazione al Piano di DR trasmesso in precedenza, specifichi le modifiche intervenute e le motivazioni di tali modifiche.

<u>La scadenza temporale per questi adempimenti è il 31/12/2012.</u>

Nella figura seguente sono rappresentate le macro-attività di avvio, implementazione e manutenzione della Continuità Operativa in modo da evidenziare l'impegno delle Amministrazioni comunali di pianificazione, progettazione, realizzazione e gestione delle soluzioni organizzative e di ICT che sottendono la produzione del Piano di Continuità Operativa e del Piano di Disaster Recovery.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Figura 1: *Adempimenti dei Comuni per l'avvio, la realizzazione e la manutenzione della Continuità Operativa.*



IL PERCORSO VERSO LA CONTINUITÀ DEI SERVIZI COMUNALI

La Continuità Operativa: una necessità per tutti i Comuni

La perdita, definitiva o temporanea, di dati strategici o sensibili inerenti all'attività di un Comune, determinati da attacchi malevoli o anche solo da inconvenienti tecnici, causa considerevoli **danni economici e conseguenze legali.** Per predisporsi ai potenziali fermi delle operatività quotidiane è necessario dotarsi di adeguati sistemi.

Attualmente molti Comuni svolgono **attività di storage/backup non conformi ai vincoli normativi e inefficaci**, limitandosi a effettuare **backup locali** (ad es. su sistemi a nastro) dei dati ritenuti più critici. Questi sistemi locali sono, inoltre, **a rapida obsolescenza, privi di fault tolerance e funzionalità di accounting**.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Senza contare che **non è praticamente mai disponibile un "ambiente di replica" remoto** subito utilizzabile in caso di fermo al fine di garantire la continuità operativa delle attività istituzionali. Le operazioni di fall-back dei dati di backup, infatti, richiedono la ricostruzione del sito originario e la nuova messa in opera dell'ambiente IT a valle del fermo nonché la risoluzione di tutti i problemi annessi, sia in termini di disponibilità/agibilità della locazione fisica, sia in termini di acquisizione delle componenti hardware necessarie, richiedendo dunque diverse settimane di tempo.

Riguardo la necessità di conservare il backup presso un sito remoto, le linee guida inquadrano le possibili soluzioni di Disaster Recovery che le PA devono adottare in relazione alle varie criticità riscontrate, in sei diverse tipologie di intervento denominate "Tier" e articolate come segue (v. anche figura successiva):

Tier1: Backup dei dati presso un altro sito tramite trasporto di supporto.

Tier2: Equivalente al Tier1 con tempi sensibilmente più brevi.

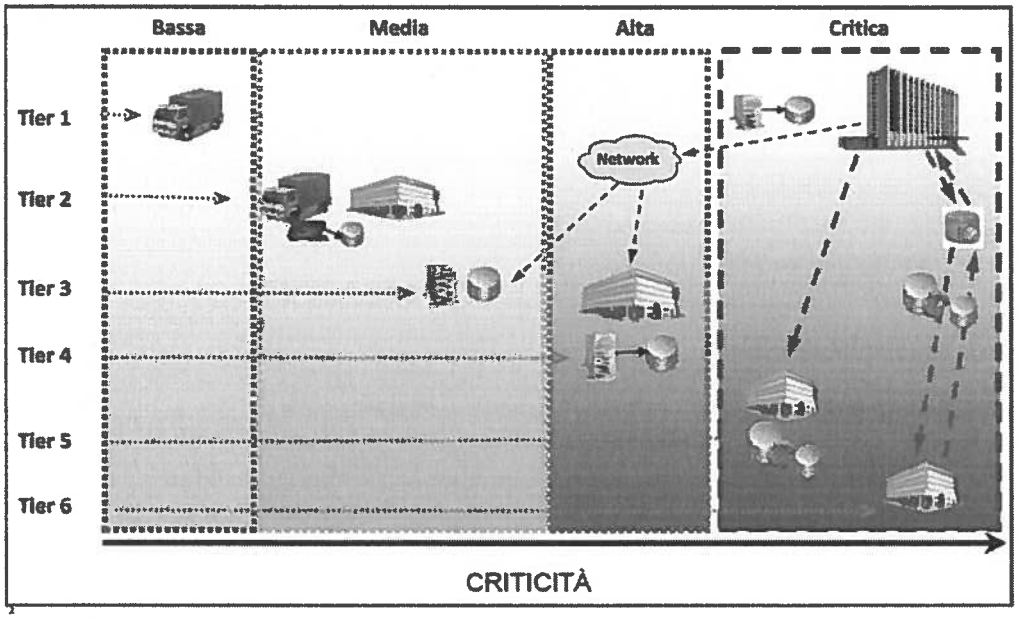
Tier3: Equivalente al Tier 2, con trasferimento dei dati attraverso un collegamento di rete tra i due siti.

Tier4: Risorse elaborative, garantite coerenti con quelle del centro primario, sempre disponibili con ripartenza delle funzionalità in tempi rapidi. Aggiornamento asincrono dei dati (RPO) con frequenza molto alta.

Tier5: Equivalente al Tier4, con aggiornamento finale dei dati quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti. Sensibile alla distanza geografica.

Tier6: Equivalente al Tier5 con risorse elaborative sempre attive e funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività dell'IT in tempi molto ristretti.

Figura 2*: Suddivisione in Tier delle soluzioni di Continuità operativa per le PA*



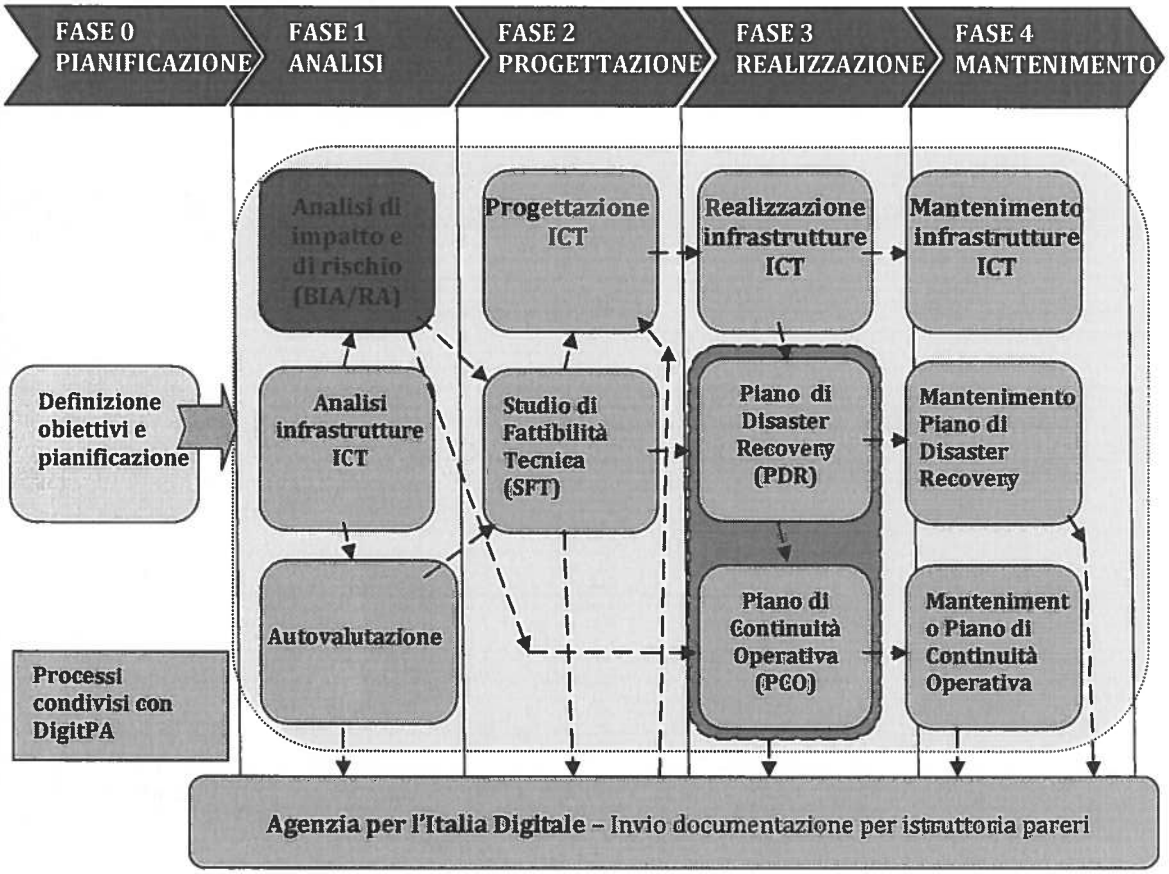
SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Il Programma e la sua articolazione in fasi

La Continuità Operativa investe diverse componenti e risorse strategiche di ciascuna Amministrazione: il management ad alto livello, le diverse strutture organizzative coinvolte nei processi di servizio (Direzioni/Uffici), le piattaforme tecnologiche impiegate.

Ciò comporta che l'Amministrazione comunale è chiamata a definire e coordinare un programma articolato in diverse fasi, che richiede il mandato dei vertici dell'Ente. Nella figura seguente viene riportato il quadro complessivo delle attività che devono essere espletate da ciascun ente.

Figura 3: *Il Programma di lavoro di un Comune*



Fase	**0**
Attività	Definizione obiettivi, ruoli, pianificazione
Output	**PROGRAMMA DI LAVORO**

È una fase significativa per la buona riuscita di tutto il programma. Per questo, essa deve caratterizzarsi con il necessario mandato dei vertici dell'Amministrazione, con la partecipazione dei responsabili dell'organizzazione e dei processi e degli addetti alla gestione dell'ICT, in modo da poter svolgere una efficace azione di programmazione e stabilire, senza approssimazione, le risorse necessarie e le modalità per reperirle.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Fase	**1**
Attività	Analisi: Valutazione dei servizi
Output	**TEST DI AUTOVALUTAZIONE**

Durante questa attività occorre procedere a:

1. Assessment IT, comprendente :
   a. la Ricognizione preliminare e strutturata dei principali asset ICT del Comune,
   b. l'Analisi delle policy di backup,
   c. l'Analisi dei fattori di rischio e l'individuazione azioni correttive (Policy di sicurezza, climatizzazione, alimentazione, collegamenti geografici, ecc),
   d. l'Analisi dei contratti di manutenzione,
   e. l'individuazione di Fornitori critici,
   f. l'Analisi delle postazioni di lavoro critiche e alle periferiche.
2. Attività di Business Impact Analysis (BIA) e Autovalutazione per:
   a. definire l'elenco dei (macro) servizi oggetto di indagine,
   b. correlarli con la struttura organizzativa,
   c. individuare i referenti per ciascun servizio,
   d. gestire la raccolta dati e le interviste ai referenti dei servizi,
   e. analizzare i rischi e stimare gli impatti,
   f. verificare le procedure alternative e gli asset non IT
   g. verificare ricicli e normalizzazione dei risultati.

Fase	**2**
Attività	Studio di fattibilità, Progettazione di dettaglio, definizione procedure di acquisizione e allestimento
Output	**STUDIO DI FATTIBILITÀ TECNICA -BUDGET -CAPITOLATI PER BENI/SERVIZI**

Durante questa attività occorre:

1. valutare l'opportunità di uniformare le soluzioni tecnologiche limitando il numero dei tier;
2. individuare le soluzioni tecnologiche, adottare il principio della semplicità, riferendosi a tecniche facilmente reperibili sul mercato anche sottoforma di servizio.

I tier 5 e 6 implicano costi molto elevati per l'allestimento ed il mantenimento e richiedono che l'intera architettura applicativa funzioni active/active e una reazione della struttura organizzativa e gestionale con tempi coerenti con RTO/RPO prossimi a zero.

Inoltre occorre tener conto anche dei seguenti elementi che influenzano significativamente le soluzioni da adottare:

1. analisi Costi/Benefici per ciascuna contromisura o soluzione tecnica individuata, indicarne i costi di acquisizione, allestimento, mantenimento;
2. rischio residuo: alcuni rischi non saranno coperti con misure preventive. Si dovrà stabilire quali misure verranno messe in campo;
3. quali servizi escludere dallo studio e per quale motivo;
4. la scelta del sito secondario: la differenziazione del rischio;
5. la scelta della connessione geografica con il sito secondario (parametri come la movimentazione giornaliera, traffico utente, limitazione accessi).

Fase	**3**
Attività	Realizzazione infrastrutture ICT, Redazione Piani di Continuità Operativa e di Disaster Recovery
Output	**PIANO DI CO – PIANO DI DR– CONTRATTI DI ACQUISIZIONE BENI/SERVIZI**

In questa fase vanno ricomprese tutte le attività per la redazione del Piano di Continuità Operativa e del Piano di Disaster Recovery e per la realizzazione della infrastruttura ICT.

Il **Piano di continuità operativa (PCO)** fissa gli obiettivi e i principi da perseguire, descrive i ruoli, le responsabilità, i sistemi di escalation e le procedure per la gestione della continuità operativa, tenuto conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche. Il piano di continuità può essere solo un documento di primo livello, cui vanno associati documenti di secondo livello, quali procedure relative a servizi e/o sistemi specifici e finanche documenti di terzo livello (per esempio sotto la forma di istruzioni di lavoro che riportano le indicazioni operative specifiche). Il PCO deve prendere in esame:

a. la definizione degli scenari valutati per il piano;
b. la definizione della struttura organizzativa che viene dedicata al governo della Continuità operativa (Comitato di crisi dell'Amministrazione, Unità di coordinamento della Continuità operativa, Gruppi di supporto);
c. l'individuazione dei criteri oggettivi per la definizione dell'evento disastroso (es.: criteri per avviare le procedure di escalation nelle diverse situazioni previste, criteri per la stima dei danni, criteri per la stima dei tempi di ritorno alla normalità "in sito", ecc);
d. la predisposizione di un template di "scheda valutazione evento";
e. la predisposizione di elenchi nominativi, ruoli e rubriche;
f. l'organizzazione della comunicazione interna e esterna e la formazione del personale del comune.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Il **Piano di Disaster Recovery (PDR)**, costituisce parte integrante del Piano di Continuità Operativa e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. In particolare il PDR deve prendere in esame:

a. le procedure organizzative per la gestione del processo di DR ovvero chi chiamare e dove recarsi;

b. le procedure tecniche gestite mediante la predisposizione di un apposito cruscotto (Processo di gestione dell'escalation e valutazione dell'evento, Fase di avvio dei servizi nel sito di Disaster Recovery, Fase di ritorno alla normalità);

c. le simulazioni;

d. l'organizzazione dei test;

e. il Piano di rientro nella normalità.

Per la **Realizzazione della infrastruttura ICT**, l'Amministrazione, a seguito dei tier che sono stati individuati nello SFT e delle soluzioni ICT che vengono elaborate nella FASE 2, deve procedere alla concreta implementazione di tali soluzioni stabilendo il "sito secondario" e avviare i test di start-up per il backup remoto delle applicazioni oggetto di Disaster Recovery.

Fase	**4**
Attività	Gestione del sistema,mantenimento
Output	**MANUALE DI GESTIONE E MONITORAGGIO**

La fase di mantenimento si riferisce alle seguenti attività:

1. mantenimento delle infrastrutture ICT;
2. mantenimento del piano di Disaster recovery;
3. mantenimento del Piano di Continuità Operativa;

In particolare le azioni che devono essere assicurate da parte del Comune sono le seguenti:

1. aggiornamento dell'Analisi BIA/RA;
2. aggiornamento delle informazioni organizzative;
3. aggiornamento elenchi, rubriche, password;
4. aggiornamento procedure (organizzative e tecniche);
5. rielaborazione dei piani;
6. pianificazione dei test (una volta ogni anno);
7. estensione del PCO a settori non presi in esame.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

IL CATALOGO DEI SERVIZI ASMECLOUD

La Continuità Operativa: una opportunità per tutti i Comuni

Il catalogo dei servizi AsmeCloud si basa sull'utilizzo di infrastrutture ICT all'avanguardia in termini di tecnologia, standard di sicurezza fisica e logica e assistenza grazie alla partnership tecnica con Telecom Italia Spa.

I servizi AsmeCloud gestiscono entrambi gli aspetti critici relativi alla continuità operativa e al disaster recovery, garantendo la conservazione remota dei dati di backup e la disponibilità di un ambiente di replica subito utilizzabile; in particolare permettono di:

1. salvaguardare in totale sicurezza e conformità i dati ritenuti più critici conservando una copia di backup degli stessi presso il Centro backup Remoto – CBR (che risiede presso il computer site di Telecom Italia);
2. garantire la continuità operativa delle attività più critiche svolte dal Comune attraverso la disponibilità di un ambiente virtuale replicato ospitato presso lo stesso CBR;
3. realizzare l'Agenda Digitale Italiana ricorrendo alla tecnologia Cloud computing e quindi svincolare il Comune dall'onere di gestire piattaforme tecnologiche complesse e a continuo rischio di obsolescenza (in particolare con il servizio Server Farm Remota – SFR);
4. focalizzare l'attenzione dei Comuni sugli aspetti organizzativi e sulla ottimizzazione dei processi piuttosto che sulle piattaforme tecnologiche.

I servizi AsmeCloud sono articolati in modo completo ed esaustivo in :

SERVIZI BASE. Comprendono il Servizio START e il Servizio Backup Replicato dei Dati - BRD e servono a coprire tutte le attività essenziali per i Comuni per realizzare la Continuità Operativa a norma del CAD. Questi Servizi sono obbligatori (mandatory) e abilitano l'Ente all'applicazione dell'Agenda Digitale.

SERVIZI AVANZATI. Comprendono il Servizio Backup Replicato dei Server - BRS e il Servizio Server Farm Remota – SFR rivolti sia ai Comuni dotati di piattaforme e applicazioni ICT evolute sia anche ai Comuni che intendono alleggerire l'onere dell'ICT, in modo da favorire un periodo di transizione verso il Cloud computing e la graduale dismissione degli apparati tecnologici.

SERVIZI DI MANTENIMENTO. Comprendono il Servizio MAN per gestire il mantenimento annuale dei Piani di CO e di DR e l'aggiornamento e l'evoluzione delle soluzioni tecnologiche.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Figura 3: *Catalogo servizi AsmeCloud*

SERVIZI BASE	Fasi del progetto di Disaster Recovery e Continuità Operativa [FASE 0 FASE 1 FASE	**Servizio START:** 1. Predisposizione dello Studio di Fattibilità Tecnica – SFT e gestione istruttorio con DigitPA
	Piano di Continuità Operativa – Piano di Disaster Recovery [Fase 3] Servizio di Disaster Recovery conforme alle Linee guida di DigitPA {Tier3- 4] con RTO Primo giorno lavorativo e RPO 24h	**Servizio Backup Replicato dei Dati - BRD:** 1. Progettazione soluzione ICT definita nello SFT 2. Piano di Disaster Recovery - PDR e Piano di Continuità Operativa -PCO e gestione istruttoria con DigitPA per il primo anno 3. Replica del Backup delle Banche Dati sul sito remoto secondario: installazione di base e configurazione software di replica sui server dell'Amministrazione, test, collaudo e prove di Disaster Recovery di Start-up 4. Test di Disaster Recovery con cadenza annuale 5. Monitoraggio del sistema
SERVIZI AVANZATI	Servizio di Disaster Recovery conforme alle Linee guida di DigitPA [Tier 5 e 6]	**Servizio Backup Replicato dei Server - BRS:** 1. Backup Remoto dei Server sul sito secondario su macchina virtuale: installazione di base e configurazione software di replica dei server e dei dati , test, collaudo e prove di Disaster Recovery di Start-up 2. Test di Disaster Recovery con cadenza annuale 3. Monitoraggio del sistema
	Servizio di Server Farm Remota	**Servizio Server Farm Remota - SFR:** 1. Messa a disposizione di macchine virtuali sul Centro backup Remoto - CBR in modo da ospitare le applicazioni ed i relativi client . 2. Soluzione di Disaster Recovery su un sito secondario del CBR [Tier 4]. 3. Cloud computing (Potenza elaborativa e storage su Hosting evoluto)
SERVIZI DI MANTENIMENTO	Servizio di mantenimento: FASE 4	**Servizio MAN (mantenimento)** 1. Mantenimento della piattaforma tecnologica 2. Mantenimento del Piano di Disaster Recovery dell'Amministrazione e comunicazioni annuali a DigitPA. 3. Mantenimento del Piano di Continuità Operativa e comunicazioni annuali a DigitPA.

Ogni Comune utente può scegliere, in modo progressivo e flessibile, il pool dei servizi da implementare, tenendo comunque conto dei vincoli normativi esistenti.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

I servizi ASMECLOUD rispondono alle esigenze delle Amministrazioni Comunali in ambito di sicurezza e Continuità Operativa secondo quanto emanato dal CAD posizionandosi almeno sulla tipologia Tier 4 della classificazione riportata nelle Linee Guida.

Conformemente alle Linee Guida del Codice dell'Amministrazione Digitale, l'obiettivo per ciascuna Amministrazione comunale consiste nell'implementare una soluzione di Disaster Recovery per i server principali, in modo da proteggere i dati trattati e garantire la continuità operativa delle attività più critiche, anche in caso di indisponibilità del sito primario, minimizzando l'investimento necessario.

A tal fine, il servizio di Disaster Recovery AsmeCloud garantisce, nella generalità dei sistemi gestiti dalle amministrazioni comunali, il raggiungimento delle seguenti funzionalità operative:

1. possibilità di lavorare con i dati replicati aggiornati alle ultime 24 ore (i.e. Recovery Point Objective- RPO pari a 24h);
2. piena disponibilità di utilizzo dell'ambiente replicato virtuale ospitato presso il Centro backup Remoto - CBR a partire dal giorno lavorativo successivo al disastro (i.e. Recovery Time Objective - RTO corrispondente al "Next Business Day");
3. possibilità di effettuare una prova annuale di Disaster Recovery;
4. copertura standard (Lun. - Ven. 8-18) dei servizi di supporto sistemistici dell'Ambiente di Recovery.

La soluzione tecnologica per realizzare il Disaster Recovery si colloca entro i livelli di funzionalità riportati nelle Linee Guida nel Tier 4, che stabilisce la necessità di disporre, per il sito secondario "*Risorse elaborative, garantite coerenti con quelle del centro primario, sempre disponibili con ripartenza delle funzionalità in tempi rapidi. Aggiornamento asincrono dei dati (RPO) con frequenza molto alta*". È convincimento comune che questa proposta possa soddisfare, nel breve – medio periodo, le necessità prese in esame nei vari SFT che sono stati presentati o sono in corso di presentazione all'Agenzia per l'Italia Digitale per il parere come prescritto dal CAD vigente.

Le Amministrazioni comunali possono concordare con i tecnici del Centro backup Remoto - CBR un diverso valore del parametro RPO , inferiore alle 24h (Es.: 12 h), nei casi in cui si ravvedono elementi di criticità particolari per talune Applicazioni informatiche del proprio sistema informativo comunale.

Le Amministrazioni possono richiedere prestazioni di Disaster Recovery che rientrano nei Tier 5 e 6, ma in tal caso devono garantire adeguati canali di comunicazione con il sito secondario messo a disposizione dal catalogo AsmeCloud.

Infine, il catalogo dei servizi AsmeCloud prevede anche il servizio completo IaaS per tutta l'infrastruttura ICT del Comune, con la possibilità di de-infrastrutturare parzialmente o totalmente il Comune, localizzando il sito primario dell'Amministrazione presso il Centro backup Remoto - CBR. Tale servizio viene denominato Server Farm Remota - SFR e viene approfondito nel seguito.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Servizi Base (mandatory)

Il servizio START consente a ciascun Comune utente di dare attuazione alle FASI 0, 1 e 2 del Programma di lavoro, in modo efficace e non oneroso tenuto conto che la gran parte della mole dell'impegno richiesto è realizzata dal supporto tecnico del Centro backup Remoto - CBR.

Il servizio START si configura come il presupposto per ogni Amministrazione comunale per fruire degli altri servizi AsmeCloud.

In particolare, l'oggetto del servizio START consiste nelle attività di predisposizione dello Studio di Fattibilità Tecnica –SFT e di gestione dell'iter istruttorio con l'Agenzia per l'Italia Digitale, seguendo un procedimento facilitato da uno schema organizzativo collaudato ed efficiente, che agevola significativamente i Comuni nella sua predisposizione in gran parte a cura del supporto del Centro backup Remoto - CBR. *Il sistema è già stato applicato a oltre 200 Amministrazioni comunali, consentendo loro di redigere lo SFT e di superare l'iter istruttorio effettuato dall'Agenzia per l'Italia Digitale ottenendo esito positivo* (consultare la sezione "Pareri emessi per la Continuità Operativa" del sito dell'Agenzia).

Il servizio Backup Replicato dei Dati - BRD, strettamente integrato con il precedente servizio START, risponde alla generalità delle esigenze delle amministrazioni comunali secondo quanto emanato dal CAD in ambito di sicurezza informatica e Continuità Operativa.

È composto dalle seguente componenti preliminari:

1. progettazione della soluzione ICT definita nello SFT, mediante la redazione di Technical report che puntualizza le misure che verranno adottate per il disaster recovery e le tecniche ICT con le quali verranno attuate;
2. redazione del Piano di Disaster Recovery - PDR e del Piano di Continuità Operativa -PCO e gestione istruttoria con l'Agenzia per l'Italia Digitale per il primo anno.

Una volte espletate le precedenti azioni preliminari, il servizio BRD consente di implementare, in modo totalmente automatico, il salvataggio (backup) e l'eventuale ripristino (restore) dei dati contenuti nei server e nei PC dell'Ente. I "dati" in questione sono rappresentati da tutte le risorse informative la cui gestione, ai fini della CO e del DR, è stata definita nel Piano di CO e di DR dell'Ente.

Il processo BRD prevede che, prima di lasciare la rete dell'Ente, i dati oggetto di Backup Replicato siano cifrati per garantire la riservatezza degli stessi, inoltre le operazioni di trasferimento da e verso il Centro Backup Remoto -CBR avvengono attraverso canali sicuri che garantiscono l'integrità e la sicurezza nella loro consegna.

In base alle specifiche caratteristiche dell'infrastruttura di cui dispone il Comune utente, viene valutato l'impiego delle soluzioni più adeguate. In taluni casi si implementa un agente software scaricabile direttamente dalla rete per eseguire le procedure di backup/restore sul Centro di BACKUP REMOTO; nelle realtà più complesse si installa un sistema di concentrazione, compressione e de-duplicazione dei dati che consente tempi di salvataggio più brevi.

SERVIZI ASMECLOUD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Una particolare attenzione è posta sul trattamento delle basi di dati, infatti tutte le operazioni legate al **Backup Replicato** non sono mai a contatto con le banche dati di produzione; il Backup Replicato, in questo caso, preleva esclusivamente la copia di salvataggio predisposta dal DBMS senza interferire in alcun modo con il database attivo. In caso di restore, la copia salvata è riportata in una posizione all'interno della rete dell'ente da cui è possibile effettuare il successivo ripristino del DBMS.

Di seguito le caratteristiche del servizio BRD:

1. i dati oggetto di Backup Remoto vengono cifrati e compressi dall'agente software installato sulla postazione e/ sul server della LAN dell'ente, prima di essere trasmessi verso il Centro backup Remoto -CBR attraverso un canale sicuro, che viene configurato dal CBR;
2. Viene garantito il servizio di monitoraggio h24 della funzionalità dell'infrastruttura tecnologica e di rete, 365 giorni all'anno;
3. Il servizio che viene offerto è indipendente dalla piattaforma applicativa e dai sistemi operativi che vengono impiegati dagli Enti nei propri domini;
4. Gli agenti di backup sono installabili su un'ampia gamma di piattaforme e sistemi operativi, di cui si riporta un elenco a titolo puramente esemplificativo:

   Applicazioni specifiche
   Windows, Linux file server
   Windows, Linux systems
   Windows XP, Vista, 7
   Microsoft Exchange
   Microsoft SQL Server
   Microsoft Sharepoint Services Foundation
   DBMS Oracle
   DBMS MySQL
   DBMS Postgress
   Sistemi Operativi
   Microsoft Windows XP SP3 (32 bit)
   Microsoft Vista SP2
   Microsoft Windows 7 SP1
   Microsoft Windows Server 2003 R2
   Microsoft Windows Server 2008 R2 SP1

5. Il servizio BRD presenta i seguenti standard :
   a. possibilità di lavorare con i dati replicati aggiornati alle ultime 24 ore (i.e. Recovery Point Objective- RPO pari a 24h);
   b. piena disponibilità di utilizzo dell'ambiente replicato virtuale ospitato presso il Centro backup Remoto - CBR a partire dal giorno lavorativo successivo al disastro (i.e. Recovery Time Objective - RTO corrispondente al "Next Business Day");
   c. possibilità di effettuare una prova annuale di Disaster Recovery;
   d. copertura standard (Lun. - Ven. 8-18) dei servizi di supporto sistemistici dell'Ambiente di Recovery (Centro backup Remoto - CBR).

2. Il servizio BRD comprende tutte le attività di avviamento e di test iniziali a carico di ASMEZ, comprese tutte le installazioni degli agenti che permettono le repliche tra siti primario (apparati dell'Ente) e sito secondario CBR.
3. Il servizio BRD non comprende l'onere della connettività tra sito dell'Ente e sito di replica (Centro backup Remoto - CBR), che rimane a carico dell'Ente.
4. Il servizio BRD consente di soddisfare le esigenze funzionali evidenziate nello SFT fino al Tier 4.

Infine si evidenzia che il servizio START e il servizio BRD rappresentano l'insieme dei servizi di base che consentono di dare concreta attuazione alla Continuità Operativa dell'Ente.

Servizi Avanzati

Il **servizio Backup Replicato dei Server - BRS** svolge oltre alle attività di backup remoto dei dati assicurati dal precedente servizio BRD, la messa a disposizione di una "Piattaforma virtualizzata di server" in modo da dare **la massima continuità operativa all'uso dei sistemi applicativi gestiti dal Comune e garantire l'erogazione di servizi "minimi" in caso di necessità**. In tal modo il Comune dispone, presso il Centro di Backup Remoto - CBR, di una copia sia dei dati che dei server in esercizio presso il proprio dominio applicativo.

Nel Centro di Backup Remoto -CBR, infatti, risiedono una serie di VM (Virtual Machine) configurate ad hoc in modo da consentire l'esercizio dei software gestionali in uso presso il Comune.

In tale ottica per ciascun Comune utente sono riservate una o più macchine virtuali. Ognuna di tali macchine virtuali è dedicata a uno o più software applicativi , in modo da consentire l'associazione logica tra server fisici installati presso ogni ente e server virtuali installati presso il CBR.

L'attività di analisi della soluzione da adottare viene condotta dai tecnici specialisti del CBR in coordinamento con il personale dell'ente.

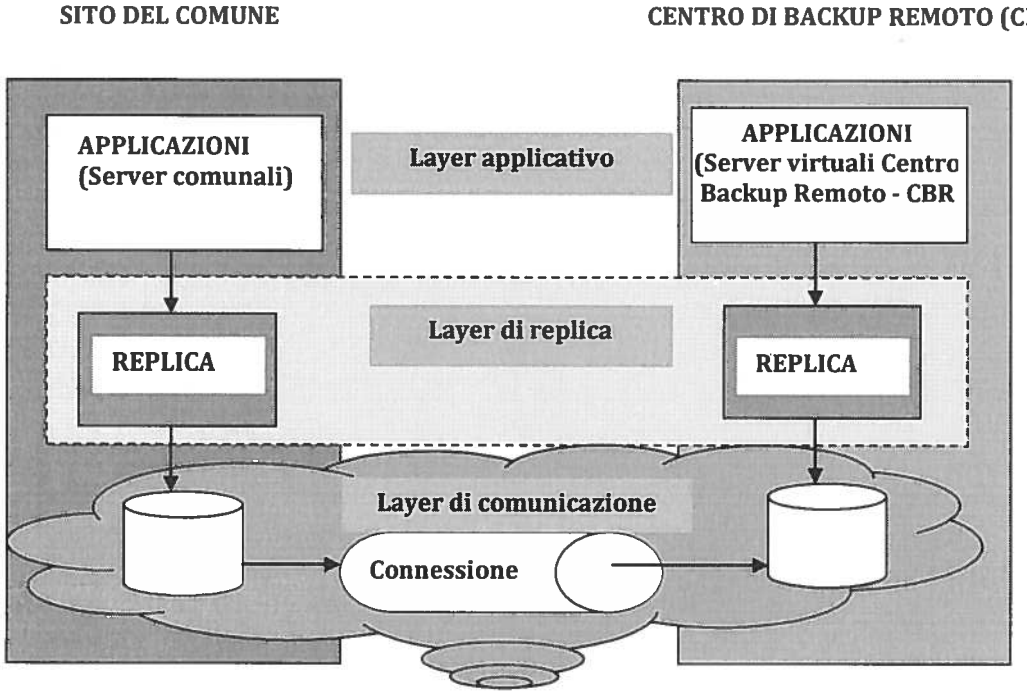
La predisposizione delle macchine virtuali e le attività di avviamento sono a carico del personale del Centro backup Remoto – CBR.

È possibile ripristinare i dati archiviati nel CBR tramite l'operazione di Backup Remoto dei Dati; in questo modo l'Ente può ripristinare i software gestionali con l'ultimo backup disponibile e tornare alla propria operatività in un tempo limitato.

Particolare importanza riveste l'allineamento delle procedure gestionali archiviate nei server virtuali del CBR con quelle esistenti nell'infrastruttura dell'ente; tale allineamento viene garantito dalla struttura tecnica del CBR che, in funzione delle varie situazioni presenti nell'ente, provvede ad aggiornare presso il CBR le versioni del software applicativo allo stesso livello di quello disponibile dell'ente.

SERVIZI ASMECLUOD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

Figura: *Schema logico- funzionale del servizio BRS*



Naturalmente, l'implementazione del servizio BRS comprende anche quella del servizio BRD, limitatamente al backup dei dati per le applicazioni condivise.

Il servizio Server Farm Remota - SFR mette a disposizione dell'Ente, presso il Centro Backup Remoto - CBR, una piattaforma per la virtualizzazione di una parte o dell'intero Sistema Informativo Comunale (sistemi server e postazioni di lavoro o client utenti).

L'implementazione del servizio sgrava il Comune da tutti gli oneri relativi all'acquisto e alla manutenzione delle macchine del Sistema Informativo Comunale, consentendo comunque di mantenere la gestione e lo sviluppo dello stesso in completa autonomia.

Vengono inoltre completamente azzerate le spese relative a:

- consumo elettrico della sala server (per una sala server di medie dimensioni circa 4-6 KW/ora per 365 giorni l'anno);
- raffreddamento della sala server e relativi servizi di manutenzione per i condizionatori;
- protezione elettrica della sala server (UPS) e relativi servizi di manutenzione;
- misure per sicurezza perimetrale, sicurezza informatica della sala server e dei singoli client.

Lo sviluppo di tecnologie per la virtualizzazione sempre più affidabili e performanti offre la concreta possibilità di "de-localizzare" i propri Sistemi Informativi Comunali in una struttura tecnica evoluta e condivisa; si ottiene così il duplice risultato di abbattere i costi di investimento, disporre di una struttura estremamente flessibile e scalabile a seconda delle esigenze del momento e soprattutto adattabile ai cambiamenti futuri.

SERVIZI ASMECLUOD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

L'ente che attiva il servizio Server farm remota -SFR accede ad un proprio cruscotto di controllo da cui il personale tecnico comunale, supportato dai tecnici del CBR, gestisce in totale autonomia le proprie VM (Macchine virtuali) e le proprie politiche di sicurezza senza nessuna limitazione.

Viene "delocalizzata" l'infrastruttura hardware e di storage e non la gestione e l'autonomia dell'ente.

Opportune policy e sistemi firewall, isolano ciascuna isola virtuale dalle altre garantendo che solo gli utenti autorizzati possano accedere a quelle risorse.

L'implementazione del servizio SFR prevede, oltre alla virtualizzazione dei server, anche la virtualizzazione delle postazioni client. Le postazioni client o utente possono essere gestite in due modalità differenti:

- *vTerminal*
  più adatta a piccole realtà, con un parco software ridotto; personalizzazione limitata all'aspetto;
- *vDesktop*
  adatta a realtà medio/grandi, personalizzazione completa fino all'installazione di software diversi in base all'utente.

Entrambe le opzioni (vTerminal e vDesktop) possono essere utilizzate sia dai normali PC sia dai più economici Thin Client che riducono drasticamente sia i consumi elettrici (PC circa 400W, Thin client 50W) sia la rumorosità (nei Thin client non ci sono ventole o altre parti in movimento).

La virtualizzazione delle postazioni di lavoro, consente di utilizzare dispositivi diversi per accedere alla stessa postazione; sarà quindi possibile accedere al proprio desktop anche tramite un dispositivo tablet o smartphone.

Infine, essendo ospitata direttamente presso il Centro backup Remoto – CBR, la Server Farm viene automaticamente sottoposta a backup sui siti di replica del CBR; in caso di necessità l'utente può accedere al sito di replica riattivare le proprie macchine ripristinando immediatamente tutte le funzionalità della Server Farm Remota.

Per l'implementazione di questo servizio il personale tecnico specialistico del Centro backup Remoto - CBR si rende disponibile per la fase di analisi e progettazione della piattaforma da realizzare e per procedere alla pianificazione e sviluppo delle attività di avviamento in parallelo, collaudo e messa in esercizio.

Il servizio che viene offerto è indipendente dalla piattaforma applicativa e dai sistemi operativi che vengono impiegati dagli Enti nei propri domini.

SERVIZI ASMECLUOD PER LA CONTINUITÀ OPERATIVA E IL DISASTER RECOVERY DEI COMUNI

A titolo esemplificativo vengono presentati alcuni esempi di piattaforme già in gestione:

Applicazioni specifiche
Windows, Linux file server
Windows, Linux systems
Windows XP, Vista, 7
Microsoft Exchange
Microsoft SQL Server
Microsoft Sharepoint Services Foundation
DBMS Oracle
DBMS MySQL
DBMS Postgres

Sistemi Operativi
Microsoft Windows XP SP3 (32 bit)
Microsoft Vista SP2
Microsoft Windows 7 SP1
Microsoft Windows Server 2003 R2
Microsoft Windows Server 2008 R2 SP1.

Servizi di mantenimento

La soluzione AsmeCloud prevede per ogni Ente, alla fine di ciascun anno di gestione del sistema di continuità operativa adottato, con esclusione del primo anno, il **servizio di Mantenimento (MAN)** del Piano di Continuità Operativa - PCO, del Piano di Disaster Recovery –PDR e di aggiornamento della piattaforma tecnologica impiegata, comprendendovi il supporto all'attività istruttoria che interessa l'Agenzia per l'Italia Digitale, come previsto dalla norma. Infatti, ciascun Comune deve inviare, entro il 31/12 di ogni anno, la versione aggiornata del Piano accompagnandolo con un documento che illustri le modifiche intervenute e le relative motivazioni.

Il servizio è previsto nella FASE 4 del piano di lavoro per la continuità operativa che ogni Ente è tenuto ad attuare e a cui si rimanda.

Tale servizio è strettamente correlato con il servizio START e in particolar modo con lo Studio di Fattibilità Tecnica - SFT [cfr FASE 2] e con il servizio BRD per ciò che si riferisce al PCO e al PDR [cfr FASE 3].

Per informazioni e per richiedere Listino e Commissione di Adesione
email: security@asmez.it
dps@asmez.it
Tel: 081-7879717; 081 - 7594519
Fax: 081-7879992