



CITTA' DI ATRIPALDA

PROVINCIA DI AVELLINO

ESTRATTO DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N. 107 del 02-07-2013

OGGETTO

APPROVAZIONE PIANO DI CONTINUITA' OPERATIVA AI SENSI DEL CODICE DELL'AMMINISTRAZIONE DIGITALE. D.Lgs. 82/2005.

L'anno duemilatrecento il giorno due del mese di luglio alle ore 19:00 nella Residenza Comunale, previo espletamento delle formalità prescritte dalla legge e dallo Statuto Comunale, si è riunita la Giunta Comunale.

Presiede la seduta: Avv. Paolo Spagnuolo in qualità di Sindaco.

Partecipa all'adunanza, nell'esercizio delle sue funzioni, il Segretario Generale Dott.ssa Clara Curto.

Intervengono:

Spagnuolo Paolo	Sindaco	P
Tuccia Luigi	Vice Sindaco	A
Iannaccone Antonio	Assessore	P
Prezioso Antonio	Assessore	P
Spagnuolo Giuseppe	Assessore	P
Tomasetti Concetta	Assessore Esterno	A

Il Sindaco, riconosciuta valida l'adunanza, dichiara aperta la seduta e la discussione sull'oggetto all'ordine del giorno.

Sulla proposta di deliberazione di cui all'oggetto ai sensi dell'art. 49, 1° comma, del D.Lgs. 267/00, come modificato dalla legge 213/12, hanno espresso i relativi pareri i responsabili dei Settori interessati come riportati in calce.

LA GIUNTA COMUNALE

Premesso che ai sensi dell'art. 50-bis del Decreto legislativo n. 82 del 07.03.2005 “Codice dell'Amministrazione Digitale” così come modificato dal D.Lgs. n. 235 del 30.12.2010, le Pubbliche Amministrazioni sono tenute a redigere adeguati piani di emergenza al fine di garantire l'operatività degli uffici e dei servizi ed il ripristino delle normali condizioni di funzionamento qualora l'organizzazione o parte di essa sia colpita da eventi distruttivi o comunque dannosi;

Che a tal fine le Pubbliche Amministrazioni sono obbligate a definire:

- a) il Piano di Continuità Operativa (PCO), che fissa gli obiettivi e i principi da perseguire, le procedure per la gestione della continuità operativa e le idonee misure preventive;
- b) il Piano di Disaster Recovery (PDR), che costituisce parte integrante di quello di continuità operativa che stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti, in siti alternativi a quelli di produzione;

Considerato che attività preliminare all'adozione del Piano di Continuità Operativa è la redazione di un dettagliato studio di fattibilità tecnica sul quale è obbligatorio acquisire il parere dell'Agenzia per l'Italia Digitale (AID ex. DigitPA);

Viste al riguardo le linee guida per il *Disaster Recovery* delle Pubbliche Amministrazioni della AID e la circolare n.58/2011 emanate sempre dalla AID per fornire alle Pubbliche Amministrazioni le direttive e i metodi attuativi per la redazione dello studio di fattibilità tecnica, il suo invio e l'acquisizione del relativo parere;

Evidenziato che questo ente ha inoltrato la richiesta di parere obbligatorio all' AID e lo SFT corredato degli esiti dell'autovalutazione eseguita mediante lo strumento di autovalutazione di cui alle “Linee Guida sul Disaster Recovery delle Pubbliche Amministrazioni”, in ottemperanza all'art. 50 bis del CAD richiamato, con il supporto tecnico e operativo del Consorzio Asmez; giusto affidamento disposto con Determina del I Settore n. 353/12;

Evidenziato, inoltre, alla richiesta di parere è stata allegata la Relazione illustrativa degli obiettivi complessivi dell'Amministrazione ai fini della digitalizzazione e dell'attuazione degli adempimenti del CAD, nonché per assicurare il rispetto delle Regole Tecniche dallo stesso CAD previste;

Considerato che questo ente ha ottenuto “Parere favorevole” dall'Autorità per l'Italia Digitale sullo SFT, risultando tra i primi comuni in Italia nella graduatoria di cui al sito dell'Autorità;

Ritenuto procedere all' approvazione del PCO Piano di Continuità Operativa e Disaster Recovery al fine di garantire continuità nella fase di start-up dei nuovi adempimenti;

Considerato che per la predisposizione, redazione, attuazione e aggiornamento dei Piani di Continuità Operativa e Disaster Recovery, le linee guida della DigitPa individuano nuovi ruoli come quello del Responsabile della Continuità Operativa, che è stato affidato all'Istruttore Direttivo Amato De Rogatis, già Amministratore di Sistema;

Ritenuto altresì costituire il Comitato di Gestione della Crisi secondo i ruoli individuati dalla AID;

Visto il parere di regolarità tecnica ai sensi dell'art. 49 D.Lgs 267/2000 del Responsabile dell'Area Amministrativa;

Visto il D.Lgs 267/2000;

Visto lo statuto dell' Ente;

Con voti unanimi e favorevoli espressi dagli aventi diritto in forma palese

DELIBERA

Per le motivazione indicate in premessa, che si intendono di seguito richiamate integralmente

- Di approvare il Piano di Continuità Operativa allegato al presente atto per farne parte integrante e sostanziale;
- Di individuare l'Istruttore Direttivo Amato De Rogatis quale Responsabile della Continuità Operativa del Comune di Atripalda ai sensi e per gli effetti del comma 3, lettera b) dell'articolo 50-bis del D.Lgs. n. 82/200;
- Di costituire il Comitato di Gestione della Crisi coadiuvato dal referente tecnico AsmeCloud composto da:

Segretario Generale
Responsabile della Continuità Operativa
Responsabile della Sicurezza ex D.Lgs 81/80
Referente AsmeCloud;

- Di precisare che i compiti del Comitato di Gestione della Crisi sono i seguenti:
 - Definizione e validazione del Piano di Continuità Operativa;
 - Valutazione delle soluzioni di emergenza e dichiarazione dello stato di crisi;
 - Avvio delle attività di recupero e controllo del loro svolgimento;
 - Rapporti con l'esterno e comunicazioni ai dipendenti;
 - Attivazione del processo di rientro, attuato da specifici gruppi operativi, continuamente monitorati dal Comitato;
 - Avvio delle attività di rientro alle condizioni normali e controllo dello svolgimento;
 - Dichiarazione di rientro;
 - Gestione di tutte le situazioni non contemplate;
 - Gestione dei rapporti interni e risoluzione dei conflitti di competenza;
 - Promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità; di dare atto che il RCO dovrà indicare al Sindaco e al Segretario Comunale ogni necessario provvedimento, intervento o spesa nell'ambito della Continuità Operativa.

Di demandare ai Responsabili di Settore dell'Ente l'adeguamento dell'assetto organizzativo di competenza che , in termini di descrizione di attività ed uffici, rappresenta uno schema base inserito nel Piano ICT.

LA STESSA GIUNTA

Rilevata l'urgenza;

Con votazione palese, unanime, espressa per alzata di mano;

DELIBERA

Di dare alla presente immediata esecuzione ai sensi dell'art. 134 – 4° comma T.U.E.L. n° 267 del 18.8.2000.



Letto, approvato e sottoscritto

Il Presidente
F.to Avv. Paolo Spagnuolo

Il Segretario Generale
F.to Dott.ssa Clara Curto

Certificato di Pubblicazione

Certificasi dal sottoscritto Segretario che, giusta relazione dell'Istruttore addetto alle pubblicazioni, copia della presente deliberazione viene affissa all'Albo Pretorio, ai sensi dell'art.124, comma 1, del D.lgs n.267 del 18/08/2000, per la prescritta pubblicazione di 15 giorni consecutivi dal 19-07-2013

Dal Municipio, li 19-07-2013

Il Segretario Generale
F.to Dott.ssa Clara Curto

ESECUTIVITA'

Il sottoscritto Segretario, visti gli atti di ufficio;

ATTESTA

Che la presente deliberazione è divenuta esecutiva il 02-07-2013

Per espressa dichiarazione di immediata esecutività (art. 134 c. 4 D.lgs n. 267/2000).

Dal Municipio, li 19-07-2013

Il Segretario Generale
F.to Dott.ssa Clara Curto

VISTO DI Regolarità tecnica

Il Responsabile del Settore
F.to Dott.ssa Italia Katia Bocchino

Per copia conforme al suo originale.

Dal Municipio, li 19-07-2013

Il Segretario Generale
Dott.ssa Clara Curto (*)

(*) firma autografa sostituita a mezzo stampa, ai sensi dell'art. 3, comma 2, del D.Lgs 39/1993

Piano di Continuita'

Operativa ICT

Comune di Atripalda

2013

Atto di approvazione	Data	Elenco di distribuzione	Sommario Modifiche
Deliberazione di Giunta Comunale		v. paragrafo	

1 Obiettivi generali

La continuità dei sistemi informativi rappresenta per le pubbliche amministrazioni, nell'ambito delle politiche generali per la continuità operativa dell'ente, un aspetto necessario all'erogazione dei servizi a cittadini e imprese e diviene uno strumento utile per assicurare la continuità dei servizi e garantire il corretto svolgimento della vita nel Paese.

Al riguardo e più in particolare l'articolo 50-bis del CAD aggiornato (che attiene alla "Continuità operativa") delinea gli obblighi, gli adempimenti ed i compiti che spettano alle Pubbliche Amministrazioni, all'Agenzia per l'Italia Digitale (AID) e al Ministro per la pubblica amministrazione e l'innovazione, ai fini dell'attuazione della continuità operativa, disponendo come segue::

"1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le PP.AA. predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio ed il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono:

a. il Piano di Continuità Operativa, che fissa gli obiettivi ed i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni.

Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b. il piano di Disaster Recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche ed organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

AID, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di Disaster Recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di AID."

1.1 Obiettivo del Piano di Continuità Operativa ICT

L'obiettivo di questo Piano di Continuità Operativa ICT (nel seguito, semplicemente PCO) è quello di definire organizzazione, procedure, mezzi tecnici che permettano all'Amministrazione di ripristinare, in caso di interruzioni di qualunque natura, i propri servizi, così come definiti nello Studio di Fattibilità Tecnica (nel seguito: SFT) che la stessa Amministrazione ha predisposto e sul quale, così come richiesto al comma 4 dell'articolo 50-bis del CAD, ha ottenuto il parere da parte dell'Agenzia per l'Italia Digitale (nel seguito AID). Il PCO ICT ha la finalità di:

- Gestire un completo e definitivo ripristino dell'operatività in caso di disastro;
- Reagire agli eventi nel modo più tempestivo possibile;
- Stabilire un flusso di comunicazione efficiente in tempi brevissimi in caso di emergenza

Si sottolinea che il Piano oggetto di questo documento si differenzia nelle finalità da altri Piani richiesti dalle normative vigenti, quali:

- Piano di Protezione Civile, secondo Ordinanza del Presidente del Consiglio dei Ministri del 28 agosto 2007, n. 3606,
- Piano di Emergenza, secondo DL 81/2008.

Si precisa, però, che il Piano è stato comunque verificato come coerente con le suddette normative.

Benché il presente Piano rappresenti una specifica realizzazione nel contesto di quanto previsto dall'articolo 50-bis del CAD e non sia, quindi, direttamente riconducibile a un preciso standard, sono norme internazionali di riferimento le seguenti:

- ISO 22301:2012 ("Societal security – Business continuity management systems – Requirements")
- ISO/IEC 27031:2011 ("Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity")
- ISO/IEC 24762:2008 ("Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services")

1.2 Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

- Il Sindaco ed il Segretario Comunale (o Direttore generale);
- il responsabile della CO ICT del Comune, così come indicato nelle “Linee guida per il DR delle PA” emesso dall’Agenzia per l’Italia Digitale il 26 novembre 2011;
- il responsabile della sicurezza dei luoghi di lavoro del Comune;
- il personale dell’Amministrazione di qualunque tipologia (fruitore o gestore) direttamente coinvolto nell’IT dell’Amministrazione;
- la comunità di riferimento territoriale e sociale (cittadini e imprese) dell’Amministrazione;
- le organizzazioni e/o istituzioni che interagiscono con l’Amministrazione in modalità informatiche;
- tutti i fornitori, a qualunque titolo, di attività di supporto informatico.

1.3 Il percorso dello Studio di Fattibilità Tecnica ex comma 4, art. 50-bis del CAD

In data 10/10/2012 l’Amministrazione ha presentato richiesta di parere, così come previsto dal comma 4 dell’articolo 50-bis del CAD.

AID ha emesso parere favorevole condizionato.

1.4 I servizi in ambito nello SFT

I servizi in ambito identificati nello SFT CON I RELATIVI LIVELLI (Tier) di criticità sono stati seguenti:

Servizio / classe servizi	Classe criticità	Sol. Tecnologica minima da autovalutazione	Soluzione tecnica individuata	Soluzione già presente	RPO	RTO
Classe1A	Media	Tier 3	Soluzione A	Backup locale su cassetta, sito DR non ancora implementato	24 Ore	30 Ore
Classe1B	Media	Tier 3	Soluzione B	I dati del sito primario sono replicati in modalità asincrona su base orario nel sito secondario	24 Ore	30 Ore
Classe 2 A	Media	Tier 3	Soluzione A	Backup locale su cassetta, sito DR non ancora implementato	24 Ore	30 Ore
Classe 2 B	Media	Tier 3	Soluzione B	I dati del sito primario sono replicati in modalità asincrona su base orario nel sito secondario	24 Ore	30 Ore

Piano di Continuità Operativa ICT

Classe3A	Media	Tier 3	Soluzione A	Backup locale su cassetta, sito DR non ancora implementato	24 Ore	30 Ore

1.5 La sintesi del parere di AID.

Esprime parere favorevole, a condizione che:

- 1) venga verificato, nell'implementazione delle soluzioni tecniche di DR descritte, che la stessa sia effettivamente in grado di rispondere alle esigenze di continuità operativa con particolare riferimento ai tempi massimi di ripristino (RTO) e di perdita massima di dati accettata (RPO);
- 2) relativamente alla soluzione tecnica "Soluzione A", venga verificato che la scelta del sito secondario sia adeguata a garantire le esigenze di continuità operativa a fronte di eventi che possano compromettere l'operatività di entrambi i siti e se ne dia riscontro nel piano di Disaster Recovery;
- 3) relativamente alla soluzione tecnica "Soluzione A", vengano individuate soluzioni tecniche di DR alternative a quella proposta, anche se di livello tecnologico (tier) inferiore, nel caso di ritardi significativi nella disponibilità della infrastruttura.

1.6 Variazioni eventuali nel numero dei servizi e relative criticità.

Servizio / classe servizi	Classe criticità	Sol. Tecnologica minima da autovalutazione	Soluzione tecnica individuata	Soluzione già presente	RPO	RTO
Classe1A	Media	Tier 3	Soluzione A	Backup locale su cassetta, sito DR non ancora implementato	24 Ore	30 Ore
Classe1B	Media	Tier 3	Soluzione B	I dati del sito primario sono replicati in modalità asincrona su base orario nel sito secondario	24 Ore	30 Ore
Classe 2 A	Media	Tier 3	Soluzione A	Backup locale su cassetta, sito DR non ancora implementato	24 Ore	30 Ore
Classe 2 B	Media	Tier 3	Soluzione B	I dati del sito primario sono replicati in	24 Ore	30 Ore

Piano di Continuità Operativa ICT

				modalità asincrona su base orario nel sito secondario		
Classe3A	Media	Tier 3	Soluzione A	Backup locale su cassetta, sito DR non ancora implementato	24 Ore	30 Ore

Prima stesura nessuna variazione

1.7 Sintesi di informazioni organizzative e tecniche sull'Amministrazione

1.8 Matrice servizi/organizzazione (responsabilità)

Classe di Servizi	Uffici	Descrizione Uffici	Tipologia di Utenza
Classe 1A	DEM_1	demografici / Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Eterogenea
Classe 1A	DEM_1	demografici / Stato civile - Attività di gestione dei registri di stato civile	Eterogenea
Classe 1A	SEG_1	Gestione atti amministrativi	Eterogenea
Classe 1A	RAG_1	Gestione finanziaria-impegni e mandati	Eterogenea
Classe 1A	MAN_1	Gestione manutenzione edifici e strade	Eterogenea
Classe 1A	SOC_1	Uff. Assistenza - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)	Aziende/cittadini
Classe 1A	SOC_1	Uff. Assistenza - Attività relativa all'assistenza domiciliare	Aziende/cittadini
Classe 1B	U. O. C. - 1° Settore	Sito web istituzionale	Eterogenea

Classe 2A	PERS_1	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune – attività relativa al riconoscimento di benefici connessi all'invalidità civile e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa	Utente Interno
Classe 2A	SOC_2	Uff. Assistenza - Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale	Aziende/cittadini

Piano di Continuità Operativa ICT

Classe 2A	SOC_2	Uff. Assistenza - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc.	Aziende/cittadini
Classe 2A	SOC_2	Uff. Assistenza - Attività ricreative per la promozione del benessere della persona e della comunità , per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	Aziende/cittadini
Classe 2A	SOC_2	Uff. Assistenza - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo	Aziende/cittadini
Classe 2A	SOC_2	Uff. Assistenza - Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale	Aziende/cittadini
Classe 2A	SOC_2	Uff. Assistenza - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Aziende/cittadini
Classe 2A	SOC_2	Uff. Assistenza - Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti	Aziende/cittadini
Classe 2A	SOC_2	Uff. Assistenza - Attività relative alla concessione di benefici economici	Aziende/cittadini
Classe 2A	SOC_2	Uff. Istruzione - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	Aziende/cittadini
Classe 2A	SOC_2	Uff. Istruzione - Attività di formazione ed in favore del diritto allo studio	Aziende/cittadini
Classe 2A	SOC_1	Cultura - Gestione biblioteca	Aziende/cittadini
Classe 2A	PM	Polizia municipale - Attività relativa all'infortunistica stradale	Aziende/cittadini
Classe 2A	PM	Polizia municipale - Gestione delle procedure sanzionatorie	Aziende/cittadini
Classe 2A	PM	Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa	Aziende/cittadini
Classe 2A	PM	Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	Aziende/cittadini
Classe 2A	PM	Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	Eterogenea
Classe 2A	SEG_2	Attività riguardante gli istituti di democrazia diretta	Eterogenea
Classe 2A	PRC	Protezione civile	Aziende/cittadini
Classe 2A	SEG_2	Conferimento di onorificenze e di ricompense	Aziende/cittadini
Classe 2A	TEC_1	Gestione edilizia privata e pratiche edilizie	Eterogenea
Classe 2a	PROTO	Protocollo Informatico	Eterogenea

Piano di Continuità Operativa ICT

Classe 2B	PROTO	Albo Pretorio Informatico	Eterogenea
Classe 2B	PM	SUAP on line	Eterogenea

Classe 3A	RAG_2	Gestione economale	Eterogenea
Classe 3A	RAG_2	Gestione finanziaria-bilancio	Eterogenea
Classe 3A	TEC_1	Progettazione	Eterogenea
Classe 3A	TEC_2	Urbanistica	Eterogenea
Classe 3A	SEG_3	Iscrizioni ad albi comunali di associazioni ed organizzazioni di volontariato	Eterogenea
Classe 3A	DEM_2	Uff. demografici / Elettorale - Attività relativa all'elettorato attivo e passivo	Aziende/cittadini
Classe 3A	DEM_2	Uff. demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio	Aziende/cittadini
Classe 3A	DEM_2	Uff. demografici / Elettorale - Attività relativa alla tenuta dell'elenco dei giudici popolari	Aziende/cittadini
Classe 3A	DEM_2	Uff. demografici / Leva - Attività relativa alla tenuta del registro degli obiettori di coscienza	Aziende/cittadini
Classe 3A	DEM_2	Uff. demografici / Leva - Attività relativa alla tenuta delle liste di leva e dei registri matricolari	Aziende/cittadini
Classe 3A	PM_2	Polizia municipale - Attività relativa al rilascio di permessi per invalidi	Aziende/cittadini
Classe 3A	SEG_3	Contenzioso – Gestione pratiche legali.	Utente Interno
Classe 3A	SOC_3	Attività ricreative, promozione della cultura e dello sport ed occupazioni di suolo pubblico	Eterogenea
Classe 3A	Servizi SOC_3	Uff. Assistenza - Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Aziende/cittadini

1.9 Matrice servizi/infrastruttura tecnologica

Indice di tecnologia	“A”	“B”	“C”	LDS (orario o disponibilità)
Indice di priorità di ripristino	Gestione “in-house” da parte dell’Ente	Gestione presso il CT “Asmecloud”	Gestione in outsourcing presso una società	

			esterna	
"1" Servizi ad alto impatto, di immediata necessità, la cui disponibilità deve essere ripristinata rapidamente al fine di gestire l'emergenza stessa	Classe 1A	Classe 1B	Classe 1C	Fino a 6 ore al giorno
"2" Servizi ad alto impatto, non necessari alla immediata gestione dell'emergenza, il cui ripristino avviene successivamente ai servizi "1"	Classe 2A	Classe 2B	Classe 2C	Fino a 6 ore al giorno
"3" Servizi ad impatto medio/basso, non necessari alla gestione dell'emergenza, il cui ripristino può avvenire alla fine dell'emergenza/in un tempo di più giorni o settimane	Classe 3A	Classe 3B	Classe 3C	Fino a 6 ore al giorno

2 Predisposizione all'emergenza

2.1 La struttura organizzativa

La struttura organizzativa che l'Amministrazione comunale ha predisposto presenta la seguente articolazione funzionale:

- 1) **Il Comitato di gestione della crisi**, le cui funzioni sono quelle stabilite dalla linee guida sulla CO.

- 2) **I dipendenti dell'ente, inseriti in un apposito elenco (Comitato Gestione dell'Emergenza)**, che devono partecipare alle attività di protezione, salvataggio e ripristino delle informazioni e dei dati in condizioni di emergenza, riportando le azioni che devono essere poste in carico a ciascuno di loro, i relativi interlocutori e le modalità da rispettare.

2.2 Comitato di crisi ICT

Le funzioni di questo organismo sono quelle stabilite dalla linee guida sulla CO. La sua composizione è formata dai seguenti soggetti:

- **Segretario Comunale**
- **Responsabile della Continuità operativa**
- **Responsabile della sicurezza ex D.Lgs. 81/08**
- **Referente AsmeCloud** (con funzioni di supporto al Comitato)

2.3 Responsabile della Continuità Operativa ICT

Svolge le funzioni l'Istruttore Direttivo Amato De Rogatis nel ruolo di responsabile della UO

2.4 Strutture tecniche

SITO PRIMARIO (*Infrastruttura ICT Amministrazione Comunale*)

La descrizione della piattaforma tecnologica che viene impiegata per l'esercizio del sito primario viene riportata nell'allegato A che riporta l'architettura e le configurazioni degli apparati di elaborazione operanti presso l'Ente nonché la dotazione di applicazioni informatiche e delle risorse informative (basi di dati) che caratterizzano il sistema informativo Comunale.

SITO SECONDARIO

CBR (Centro di Backup Remoto) presso Asmecloud.

Il Centro Backup Remoto (o Sito Secondario) è composto da due data center (Nodo primario e secondario).

Il supporto tecnico del Centro backup Remoto - CBR mantiene apparecchiature sempre attive, condivise e non ad uso esclusivo di un singolo ente. Il Comune ha uno spazio storage riservato per la replica notturna di tutti i dati. Sono presenti macchine virtuali su cui installare in caso di necessità gli applicativi gestionali dell'ente e delle postazione client erogate in modalità terminal server raggiungibili dai dipendenti comunali tramite VPN.

Per l'implementazione dei sistemi utilizza la piattaforma OpenStack: un sistema operativo cloud che controlla un insieme di risorse computazionali, storage e di rete presenti nel data center in forma virtualizzata, tutte gestite utilizzando una dashboard che fornisce il controllo completo all'amministratore e inoltre, attraverso l'utilizzo di un'interfaccia web, offre all'utente funzionalità di self-service provisioning.

La scelta della piattaforma di virtualizzazione è di tipo misto per consentire la gestione dei diversi ambienti e semplificare ulteriormente l'integrazione. Il sistema consente di virtualizzare anche i desktop (o almeno le postazioni più critiche) per arrivare a una amministrazione comunale il più possibile ICT free. In termini di economicità la virtualizzazione permette topologicamente di integrare le piattaforme delle cinque aggregazioni in un'unica piattaforma logica facilitandone e ottimizzandone la gestione.

Nella configurazione attuale il Nodo Primario è costituito dalle seguenti apparecchiature principali:

- N. 37 Server con doppi processori (multicore) e componenti ridondati;
- N. 2 sistemi di storage (produzione e replica locale) tipo SAN in configurazione ridondata, ciascuno con capacità raw da 180 Tbyte.
- N. 1 unità Tape Library con capacità di backup in linea da circa 150 Tbyte.
- Apparati di rete ridondati e ad alte prestazioni.

Il Nodo secondario ha funzione di Disaster Recovery del primario e pertanto replica a livello di funzionalità l'intera infrastruttura hardware e software disponibile nel sito primario anche se la capacità elaborativa è dimensionata a circa il 30% di quella del sito primario.

La capacità di storage del sito secondario è la stessa di quello primario escluso il fatto che non utilizza una replica locale.

Per la replica dei dati e delle macchine virtuali dal sito primario sul sito secondario si utilizza una modalità asincrona effettuata tramite il software di replica remota dello storage.

Il Nodo Secondario è costituito dalle seguenti apparecchiature principali

- N. 12 Server con doppi processori (multicore) e componenti ridondati;
- N. 1 sistema di storage tipo SAN in configurazione ridondata con capacità raw da 180 Tbyte.
- N. 1 unità Tape Library con capacità di backup in linea da circa 150 Tbyte.
- Apparati di rete ridondati e ad alte prestazioni.

Il collegamento dei Nodi Primario e Secondario è garantito rispettivamente da un canale da 100 mbps simmetrico (banda garantita) per il sito primario e 50 mbps simmetrico (banda garantita) per il sito secondario.

2.5 Composizione, ruoli, procedure operative

I soggetti coinvolti sono i seguenti:

Ufficio	Ruolo	Descrizione ruolo	Figura Professionale	Responsabilità
<i>Responsabil e CO e DR (U.O.C. 1° Settore)</i>	<i>Responsabile Sistemi Informativi</i>	<i>Coordina e verifica la struttura tecnica legata alla gestione delle informazioni, alla corretta configurazione e gestione dell'hardware</i>	<i>Istruttore Direttivo</i>	<i>Responsabile dell'attuazione del piano di DR</i>
<i>Segretario Comunale</i>	<i>Segretario Comunale</i>	<i>Coordina i Responsabili di settore o Area</i>	<i>Segretario Comunale</i>	<i>Coordina i Responsabili di Settore e Impartisce idonei obiettivi per la gestione della Crisi</i>
<i>Ufficio Servizi</i>	<i>Responsabile</i>	<i>Gestione delle Risorse finanziarie per</i>	<i>Responsabile</i>	<i>Responsabilità: Adeguare le disponibilità di bilancio</i>

<i>Finanziari ed Economale</i>	<i>II Settore</i>	<i>fronteggiare la Crisi e rientrare dall'emergenza</i>		<i>per far fronte agli oneri della CO ICT</i>
<i>Ufficio Tecnico</i>	<i>Responsabile III Settore</i>	<i>Gestione delle infrastrutture logistiche</i>	<i>Responsabile</i>	<i>Responsabile delle strutture logistiche impianti e cablaggi. Verifica la corretta erogazione delle forniture elettriche</i>
<i>Tecnici Centro DR&BC</i>	<i>Direttore Responsabile centro tecnico presso ASMECLOUD</i>	<i>Coordina i tecnici nell'attivazione del sito DR, coordina le procedure e tempi per il rientro dell'emergenza</i>	<i>Direttore</i>	<i>Responsabile delle operazioni tecniche e di gestione del sito secondario dall'attivazione al suo rientro</i>

2.6 Gestione delle reperibilità

Reperibilità del comitato gestione di emergenza e dei soggetti coinvolti nelle operazioni di ripristino dei servizi.

Il regolamento comunale sulla CO prevede l'estensione dell'istituto della reperibilità, nella situazione di annuncio delle condizioni di emergenza, a tutti i dipendenti comunali richiamati nell'elenco di cui al precedente paragrafo. Tale istituto, su disposizione del Comitato di crisi, può essere esteso anche ad altri dipendenti o collaboratori.

Nei rapporti con i fornitori esterni di servizi ICT interessati all'esercizio delle procedure applicative e dei servizi ICT viene prevista una integrazione contrattuale con la quale si dispongono termini e condizioni dell'intervento di supporto per la gestione dell'emergenza ICT.

3 Soluzione di continuità-Ricognizione sulle infrastrutture ICT dei Comuni

3.1 Procedura di emergenza

3.1.1 Criteri di sicurezza ed Valutazione dell'emergenza

La valutazione dell'emergenza è classificata in base alla criticità e livello di impatto sull'amministrazione

CRITICITÀ DI LIVELLO 1	Le applicazioni che rientrano in questa classificazione, e che sono di seguito elencate, influenzano direttamente l'Amministrazione ed eventuali malfunzionamenti possono portare significativi danni di immagine, economici e legali.
CRITICITÀ DI LIVELLO 2	Le applicazioni che rientrano in questa classificazione, e che sono di seguito elencate, influenzano direttamente il buon andamento dell'ente, ma non sono servizi critici che possono comportare un danno alla sicurezza o salute pubblica.
CRITICITÀ DI LIVELLO 3	Le applicazioni che rientrano in questa classificazione, e che sono di seguito elencate, aiutano a far funzionare i processi interni

Piano di Continuità Operativa ICT

dell'Amministrazione. In generale un periodo di fermo è recuperabile.

Nello Studio di Fattibilità Tecnica i servizi erogati sono stati suddivisi in tre classi distinte valutando principalmente la criticità dovuta alla garanzia di esistenza in vita priorità/urgenza nel ripristino del servizio previsto dalla normativa e dalla sensibilità e quantità dei dati trattati.

Alla “**classe 1**” appartengono tutti quei servizi indispensabili per far fronte a qualsiasi tipo di minaccia ed evento che comprometta i sistemi informativi ospitati nel sito primario dell'ente.

La “**classe 2**” raccoglie i servizi ad alto impatto, ma ripristinabili in tempi successivi rispetto alla gestione dell'emergenza. Anche per questa classe di servizi, si distinguono le 3 categorie in base alla tecnologia di impianto.

Alla “**classe 3**” vengono riportati tutti quei servizi che possono per loro natura essere ripristinati anche in più giorni/settimane, pur garantendo la continuità del servizio anche attraverso l'uso di procedure alternative

La classificazione ha prodotto il seguente risultato:

CLASSE 1

Ufficio	Descrizione Uffici
DEM_1	Uff. demografici / Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)
DEM_1	Uff. demografici / Stato civile - Attività di gestione dei registri di stato civile
SEG_1	Gestione atti amministrativi
RAG_1	Gestione finanziaria-impegni e mandati
MAN_1	Gestione manutenzione edifici e strade
SOC_1	Uff. Assistenza - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)
SOC_1	Uff. Assistenza - Attività relativa all'assistenza domiciliare
U.O.C. 1° Settore	Sito web istituzionale

CLASSE 2

Ufficio	Descrizione Uffici
PERS_1	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune – attività relativa al riconoscimento di benefici connessi all'invalidità civile e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa
SOC_2	Uff. Assistenza - Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale
SOC_2	Uff. Assistenza - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc.
SOC_2	Uff. Assistenza - Attività ricreative per la promozione del benessere della persona e della comunità ,

Piano di Continuità Operativa ICT

	per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale
SOC_2	Uff. Assistenza - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo
SOC_2	Uff. Assistenza - Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale
SOC_2	Uff. Assistenza - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto
SOC_2	Uff. Assistenza - Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie
SOC_2	Uff. Assistenza - Attività relative alla concessione di benefici economici
SOC_2	Uff. Istruzione - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie
SOC_2	Uff. Istruzione - Attività di formazione ed in favore del diritto allo studio
SOC_1	Cultura - Gestione biblioteca
PM	Polizia municipale - Attività relativa all'infortunistica stradale
PM	Polizia municipale - Gestione delle procedure sanzionatorie
PM	Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa
PM	Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria
PM	Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza
SEG_2	Attività riguardante gli istituti di democrazia diretta
PRC	Protezione civile
SEG_2	Conferimento di onorificenze e di ricompense
TEC_1	Gestione edilizia privata e pratiche edilizie
PROTO	Protocollo Informatico
PROTO	Albo Pretorio Informatico
PM	SUAP on line

CLASSE 3

Ufficio	Descrizione Uffici
RAG_2	Gestione economale
RAG_2	Gestione finanziaria-bilancio
TEC_2	Progettazione

TEC_2	Urbanistica
SEG_3	Iscrizioni ad albi comunali di associazioni ed organizzazioni di volontariato
DEM_2	Uff. demografici / Elettorale - Attività relativa all'elettorato attivo e passivo
DEM_2	Uff. demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio
DEM_2	Uff. demografici / Elettorale - Attività relativa alla tenuta dell'elenco dei giudici popolari
DEM_2	Uff. demografici / Leva - Attività relativa alla tenuta del registro degli obiettori di coscienza
DEM_2	Uff. demografici / Leva - Attività relativa alla tenuta delle liste di leva e dei registri matricolari
PM_2	Polizia municipale - Attività relativa al rilascio di permessi per invalidi
SEG_3	Uff. Contenzioso – Gestione pratiche legali.
SOC_3	Attività ricreative, promozione della cultura e dello sport ed occupazioni di suolo pubblico
SOC_3	Uff. Assistenza - Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori

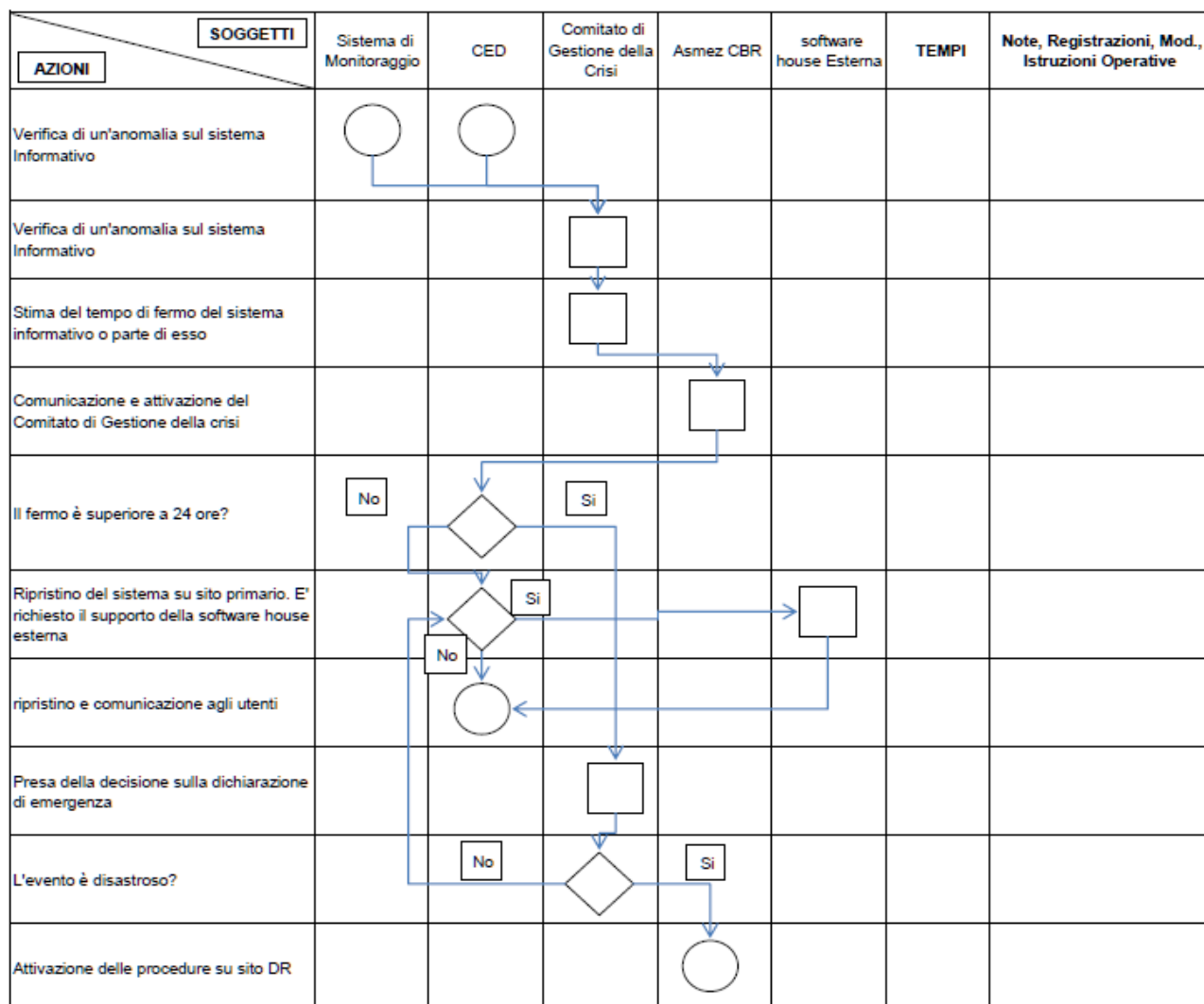
3.1.2 Comunicazioni (Lista dei contatti in caso di disastro, modalità di contatto)

Le modalità di contatto per l'attivazione del sito DR sono definite contrattualmente fra Amministrazione Comunale e CBR Asmecloud. Le procedure interne all'ente sono stabilite direttamente dal regolamento interno. I componenti del Comitato di gestione della crisi sono figure dirigenziali, quindi sempre reperibili, o comunque soggette a reperibilità attribuita con la nomina a Componente del Comitato di Gestione della Crisi. Il personale tecnico sarà contattato attraverso l'elenco dei tecnici reperibili.

3.1.3 Attivazione del piano di disaster recovery

La procedura di attivazione viene innescata ogni qualvolta si presenta una anomalia che può dar luogo ad una situazione di disastro descritta secondo la tabella riportata nel paragrafo 3.1.1. La sequenza delle comunicazioni prevede l'attivazione del processo di gestione concordato contrattualmente con il fornitore del servizio di CBR Asmecloud che prevede le seguenti fasi:

Piano di Continuità Operativa ICT



3.1.4 Scenari di emergenza applicabili e valutazione dei danni

Gli scenari individuati durante lo studio di fattibilità ci consentono di garantire dei livelli RTO e RPO per classi omogenee di servizi predefiniti nella classificazione riportata nel paragrafo 3.1.

La soluzione tecnologica scelta dall'amministrazione è definita secondo le linee guida pari al TIER 3, l'implementazione attuale della soluzione tecnica prevedere dei tempi di RPO pari a quanto dichiarato nello studio di fattibilità mentre i tempi RTO sono maggiori.

Servizio/ Classe di Servizi	RTO	RPO
Classe 1	1 settimana in caso di distruzione di server fisici o sito primario	1 giorno lavorativo
	2 giorni in caso di corruzione o distruzione dei soli dati	
Classe 2		1 giorno lavorativo
Classe 3		1 giorno lavorativo

3.1.5 Procedure di acquisto in emergenza

Le procedure di acquisto in emergenza sono attivabili secondo quanto indicato nel regolamento interno dell'Ente. Tutti gli acquisti sono definiti e valutati dal Comitato di gestione della crisi

3.1.6 Documentazione delle attività svolte (reporting)

Tutte le attività di gestione e manutenzione del sistema effettuate dai tecnici del CBR ASMECLOUD sono documentate mediante un dettagliato verbale, sottoscritto dall'amministrazione e dal direttore tecnico che certifica l'esito dell'intervento. I dati minimi riportati nel documento sono definiti nelle istruzioni operative della procedura di gestione e manutenzione e comprendono almeno: la data, l'ora, il luogo dello svolgimento del test, le figure che vi hanno partecipato, le prove svolte e l'esito.

In caso di insuccesso parziale o totale dei test, l'Amministrazione deve esaminare le problematiche emerse e attivare le azioni necessarie per la loro risoluzione.

In tal caso il verbale dei risultati dei test indicherà le azioni da intraprendere per la rimozione degli eventuali problemi riscontrati nel corso dei test unitamente alla persona o struttura incaricata di rimuoverli e alla scadenza prevista.

Tutti i verbali ovvero, il verbale di collaudo e quelli relativi ai test periodici svolti, fino al termine di vigenza della soluzione di continuità operativa e o del contratto che affida a CBR ASMECLOUD l'avvio, la realizzazione, la gestione e la manutenzione e verifica/test della soluzione, sono conservati dal CBR Asmecloud con le modalità di legge previste.

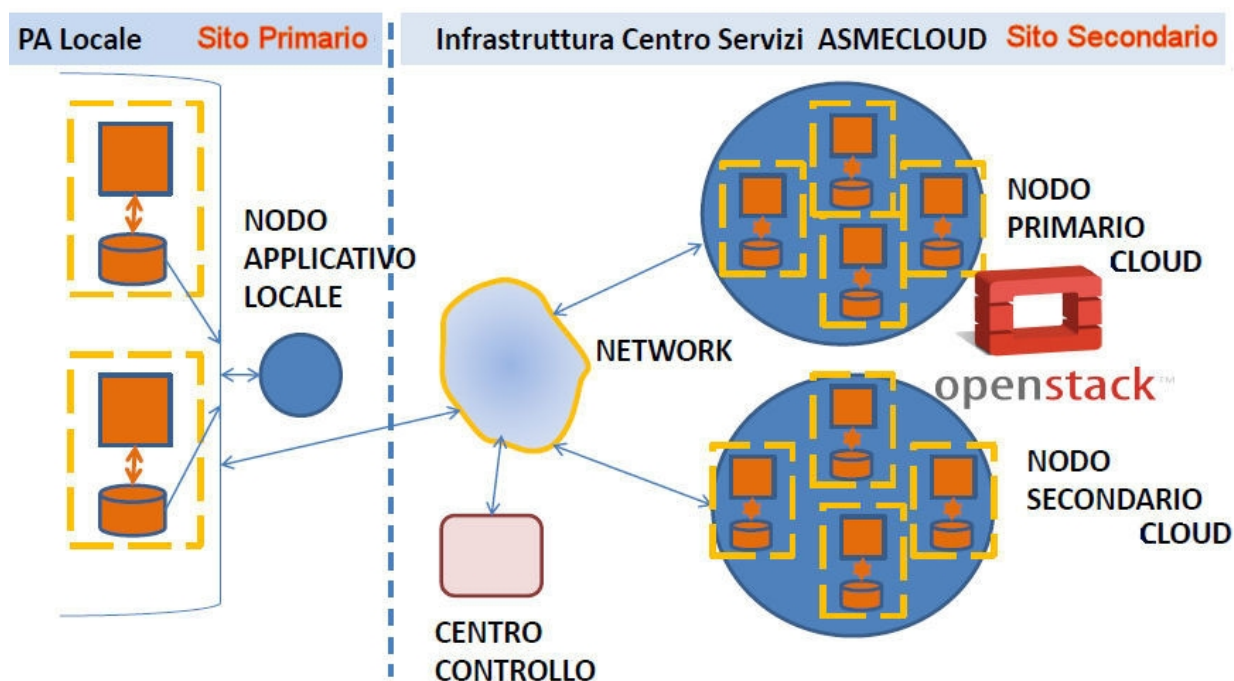
3.2 Procedure di avviamento del sito secondario

3.2.1 Preparazione del sito di disaster recovery

Il supporto tecnico del Centro backup Remoto - CBR mantiene apparecchiature sempre attive, condivise e non ad uso esclusivo di un singolo ente. Il Comune ha uno spazio storage riservato per la replica notturna di tutti i dati secondo delle logiche incrementalmente dettagliate nel seguito, inoltre sono presenti 2 macchine virtuali su cui installare in caso di necessità gli applicativi gestionali dell'ente e delle postazione client erogate in modalità terminal server raggiungibili dai dipendenti comunali tramite VPN.

Nel caso di una emergenza nel Sito Primario, per cui si renda necessario la ripartenza dei servizi dal CBR, tutte le apparecchiature ivi presenti e destinate all'utilizzo dell'Ente, sono attivate al fine di completare lo switch dei due centri. E' possibile attivare anche l'erogazione di una sola parte dei servizi danneggiati:

Schema logico dell'infrastruttura



I dati prima di essere trasferiti nel sito DR (Sito Secondario) vengono raccolti e aggregati in un dispositivo locale su cui è installato un agente di backup connesso all'infrastruttura DR attraverso un canale VPN.

I dati raccolti nel dispositivo di backup locale sono

- File ed archivi (doc, xls, p7m, mdb, pdf, dwg, ecc.)
- Backup consolidati prodotti dagli applicativi software presenti nell'ente

Da tali aree di deposito locale i file vengono trasferiti giornalmente nell'area di storage riservata al Comune presso il sito DR; per ottimizzare il traffico sulle linee dati vengono utilizzati opportuni strumenti software che consentono di implementare politiche incrementalmente nel trasferimento dei dati.

Il ripristino dei servizi e degli archivi sono a cura del Responsabile CED interno al Comune, il quale si avvarrà del supporto delle software house che forniscono gli applicativi gestionali.

Tutte le operazioni di backup sono gestibili e monitorate attraverso l'uso di un software che esegue giornalmente l'inoltro dei log sulle operazioni notturne di trasferimento dati dal sito primario al sito secondario. Il Responsabile della corretta gestione dei procedimenti di replica e verifica della reale consistenza dei dati nel sito secondario è individuato nel Responsabile della CO del Comune di Atripalda.

Livelli di Servizio

RPO	1 giorno: Dati consolidati riferiti al giorno precedente rispetto all'evento disastroso
RTO	Questo indicatore varia a seconda dell'evento disastroso: - Riferito alla distruzione dell'intero sito primario è pari a 5 giorni lavorativi - Riferito alla perdita di parte di File o Archivi o parte delle banche dati gestionali è pari a 3 giorni lavorativi

Procedura Operativa P.PSDR.01

AZIONI SOGGETTI	Comitato di Gestione della Crisi	CED	TEMPI	Note, Registrazioni, Mod., Istruzioni Operative
Il Comitato di Gestione della Crisi vista la Situazione di Crisi sceglie di attivare il sito DR				
Verifica della sistemazione e validazione delle Azioni da intraprendere				Il Responsabile della CO dell'ente adotta le decisioni intraprese dal Comitato di Gestione della Crisi
Attivazione delle procedure di verifica di dati disponibili presso il CBR,				
Check della consistenza dei dati				
Procedura di ripristino dell'infrastruttura				Procedura Operativa P.PSDR.02
Procedura di ripristino della banche dati				Procedura Operativa P.PSDR.03
Procedura di ripristino delle applicazioni				Procedura Operativa P.PSDR.04
Procedura per la gestione dell'organizzazione logistica e coordinamento del personale				Procedura Operativa P.PSDR.05
check Finale del Sito DR Secondario				
Redazione e Sottoscrizione del Verbale ed inoltro al Comitato di Gestione della Crisi				
Configurazione delle Postazioni Client Presso L'Ente				
Ripresa della Attività Operative dal parte degli operatori dell'ente				

3.2.2 Procedura di ripristino dell'infrastruttura nel Sito Secondario

Il Sito Secondario dispone di un'area riservata alla replica di tutti i dati dell'ente sia essi file o archivi che backup consolidati dei dati gestiti dagli applicativi software.

Il Comune di Atripalda dispone almeno di 2 server

Procedura Operativa P.PSDR.02

Tipo VM	Descrizione	Responsabilità
Server Applicativo	Server su cui installare le procedure gestionali e le relative share di rete	Il CBR Asmecloud avrà il Compito di mantenere e rendere disponibile la VM, vigilare sulla corretta procedura di backup durante il periodo del suo utilizzo. Inoltre dovrà garantire la disponibilità di connettività sul Sito Secondario ed il servizio di VPN. I responsabili tecnici dell'ente hanno il compito di gestire in maniera autonoma e/o con il supporto dei propri tecnici esterni specialistici tutte le operazioni di attivazione del sito, installazione e configurazione del server, nonché il restore dei dati
Client virtuali	Server dedicato all'erogazione dei servizi di Client Virtuali fruibili in modalità Terminal Server	Il CBR Asmecloud avrà il Compito di mantenere e rendere disponibile la VM, vigilare sulla corretta procedura di backup durante il periodo del suo utilizzo. Inoltre dovrà garantire la disponibilità di connettività sul sito secondario e il servizio di VPN. I responsabili tecnici dell'ente hanno il compito di gestire in maniera autonoma e/o con il supporto dei propri tecnici esterni specialistici tutte le operazioni di installazione delle postazioni client sia sul Sito Secondario che sui client fisici presenti all'interno dell'ente.

Nel Comune sono state individuate 2 postazioni di lavoro operativi in caso di emergenza per ogni Servizio erogato appartenente alla CLASSE 1 e 2 descritto nel paragrafo 3.4.

In caso di interruzione dei servizi di connettività sul Sito Primario sarà attivato un collegamento Internet su rete mobile con le opportune garanzie di sicurezza del canale (VPN).

3.2.3 Procedura di ripristino delle banche dati nel sito secondario

La procedura di ripristino delle banche dati tiene in considerazione due diverse situazioni a seconda dell'entità dell'evento e tipologia dei dati:

Procedura Operativa P.PSDR.03

Tipo di banca dati	Descrizione	Responsabilità
File e Archivi	I File / Archivi gestiti dai software di Office Automation vengono ripristinati dal software di replica a partire dalle copie disponibili nelle aree di backup del Sito Secondario. I file sono resi disponibili, con le opportune policy di sicurezza, attraverso il Client Remoto o tramite condivisione SMB.	Il CBR Asmecloud avrà il Compito di mantenere e rendere disponibile la VM, vigilare sulla corretta procedura di backup durante il periodo del suo utilizzo. Inoltre dovrà garantire la disponibilità di connettività sul Sito Secondario ed il servizio di VPN. I responsabili tecnici dell'ente hanno il compito di gestire in maniera autonoma e/o con il supporto dei propri tecnici esterni specialistici tutte le operazioni di ripristino dei file e/o archivi e la corretta configurazione delle policy di sicurezza.
Database strutturati di procedure applicative	I backup consolidati delle banche dati sono trasferiti nella VM dei servizi applicativi e ripristinati secondo le specifiche modalità dettate dalle software house, soprattutto con riferimento alle situazioni di BD in formato proprietario o DBMS specifici.	Il CBR Asmecloud avrà il Compito di mantenere e rendere disponibile la VM, vigilare sulla corretta procedura di backup durante il periodo del suo utilizzo. Inoltre dovrà garantire la disponibilità di connettività sul sito secondario ed il servizio di VPN. I responsabili tecnici dell'ente hanno il compito di gestire in maniera autonoma e/o con il supporto dei propri tecnici esterni specialistici tutte le operazioni di ripristino delle banche dati.

3.2.4 Procedura di ripristino delle applicazioni nel sito secondario

Procedura Operativa P.PSDR.04

Il responsabile della Continuità operativa e Responsabile CED del Comune Atripalda avvalendosi della collaborazione dei tecnici comunali interni o dei tecnici esterni tutti i software applicativi utili nelle attività ordinarie. L'elenco dei software e procedure di installazione necessarie per garantire i servizi in caso di emergenza sono individuate in base alla gravità ed entità dell'evento disastroso.

3.2.5 Procedura per la gestione dell'organizzazione logistica e coordinamento del personale

La procedura definisce le attività da compiere per fronteggiare una prima fase di emergenza indipendentemente dalla gravità dell'evento disastroso.

Procedura Operativa P.PSDR.05

Tipo di Evento	Evento	Azione	Responsabilità	Ordine di esecuzione e Priorità
Infrastrutture fisiche (edifici)	Distruzione completa o parziale o inagibilità di alcune aree fisiche	Individuazione di un sito alternativo	Comitato di Gestione della Crisi /Resp. Ufficio Tecnico	1 – ALTA
Infrastrutture fisiche (edifici)	Distruzione completa o parziale o inagibilità di alcune aree fisiche	Predisposizione di connessione dati ai sistemi informativi centrali del Sito Primario o di connessione con il sito DR (Sito Secondario)	Comitato di Gestione della Crisi /Resp. Ufficio Tecnico/ Resp. CED	2 - ALTA
Infrastrutture fisiche (edifici)	Distruzione completa o parziale o inagibilità di alcune aree fisiche	Dotazione di postazioni informatiche, adeguate al collegamento con il sito DR, ad un nucleo di personale dell'ente individuato come necessario per fronteggiare la crisi.	Comitato di Gestione della Crisi /Resp. CED	3 - ALTA

3.3 Ripristino del sito di produzione

3.3.1 Condizioni per il ritorno al sito di produzione

Il piano di ripristino dei sistemi sul sito primario ha l'obiettivo di documentare tutte le procedure previste per ripristinare i sistemi e i ritornare ad una normale operatività.

Generalmente viene predisposto quando tutte le facilities presenti sono state ripristinate e sono in grado di supportare tutte le funzionalità previste in precedenza.

L'attività di rientro al CED Primario di produzione viene concordata e pianificata dal Comitato di Gestione della crisi.

Una volta che l'infrastruttura del CED Primario risulterà ripristinata e pronta ad accogliere il ritorno dei sistemi, si procederà alla realizzazione dei seguenti passi:

- a) Identificazione del primo periodo utile per la migrazione. Ove possibile si preferirà la pianificazione dell'attività durante un week-end
- b) Comunicazione all'utenza della indisponibilità dei servizi per circa 48h.
- c) Disabilitazione degli accessi ai sistemi del sito primario da parte della rete geografica.
- e) Esecuzione procedure di salvataggio dell'intero ambiente dati online su supporto magnetico adatto al successivo ripristino nel sito primario (stimata in circa 8 ore).
- e) Trasporto fisico dati di salvataggio dal Sito secondario a quello primario (stima 4 ore)
- f) Ripristino dati sui dischi del sistema del CED Primario (stima 8 ore)
- g) Riattivazione sistemi e verifiche di funzionalità (stima 3 ore)
- h) Ripristino delle normali policy di accesso ai sistemi dalla rete geografica.

Procedura Operativa P.RSP.01

SOGGETTI AZIONI	Comitato di Gestione della Crisi	CED	TEMPI	Note, Registrazioni, Mod., Istruzioni Operative
Adozione della decisione di ripristino del sito primario				
Verifica della situazione e Coordinamento con il Comitato di Gestione della Crisi				
Check della situazione nel Sito Primario				
Check sullo stato attuale delle risorse, dati, procedure applicative nel sito Secondario e Stima della Mole di Dati da trasferire nel sito Primario				Scelta della modalità di Trasferimento dati dal sito secondario al sito primario
Pianificazione del Week-End per Eseguire il ripristino				Il Responsabile della CO e Responsabile CED Pianifica le attività con i Propri collaboratori e con il Comitato di Gestione della Crisi le attività di comunicazione verso la cittadinanza e dipendenti
Esecuzione delle Copie dell'intero Ambiente Secondario per poter essere trasferito nel sito Primario				
Trasferimento dei Dati dal Sito Secondario al Sito Primario				Procedura Operativa P.RSP.02
Procedura di ripristino dell'infrastruttura				Procedura Operativa P.RSP.03
Procedura di ripristino della banche dati				Procedura Operativa P.RSP.04
Procedura di ripristino delle applicazioni				Procedura Operativa P.RSP.05
check Finale del Sito Primario				
Configurazione delle Postazioni Client Presso L'Ente				
Ripresa della Attività Operative dal parte degli operatori dell'ente nel Sito Primario				

3.3.2 Procedura per il trasferimento dei dati dal sito secondario al sito primario

La procedura di trasferimento dati varia a seconda della mole di dati di trasferire fra i due siti.

Procedura Operativa P.RSP.02

Perdita completa del sito primario	Il trasferimento dati dal sito secondario al sito primario avviene tramite il recupero fisico del supporto contenente il backup completo di tutti i dati modificati sul sito secondario durante l'emergenza ed il ripristino sul sito primario.		
Perdita parziale del sito primario	A seconda della criticità ed importanza del servizio vengono adottate le seguenti procedure		
	Criticità del Servizio definita paragrafo 10.1	Quantità espressi in GB	Modalità di ripristino
	Classe 1	Superiore a 20 GB	Recupero del supporto fisico contenente il backup completo dal sito secondario al sito primario
	Classe 1	Inferiore 20 GB	Trasferimento via rete xDSL dei dati dal sito secondario al dispositivo locale di backup
	Classe 2 e Classe 3	Superiore a 50 GB	Recupero del supporto fisico contenente il backup completo dal sito secondario al sito primario
	Classe 2 e Classe 3	Inferiore 50 GB	Trasferimento via Rete xDSL delle informazioni dal sito secondario al dispositivo locale di backup

3.3.3 Procedura Ripristino dell'infrastruttura nel sito primario

Il ripristino del sito primario prevede la verifica della corretta configurazione degli apparati hardware e software prima di eseguire qualsiasi operazione di ripristino delle banche dati:

Procedura Operativa P.RSP.03

Sicurezza Fisica	- Verifica della continuità elettrica e climatizzazione dei locali adibiti ad ospitare gli apparati server e storage; - Verifica del corretto ripristino dell'hardware o collaudo dell'eventuale nuovo hardware acquistato; - Verifica di tutte le postazioni client danneggiate;
Sicurezza Logica	- Verifica di tutte le configurazioni e policy di sicurezza dell'ente;
Connettività e Connessioni dati	- Check della connessione internet e/o SCP; - Verifica della corretta configurazione di tutti gli apparati di rete interni;

3.3.4 Procedura Ripristino della banche dati nel sito primario

Procedura Operativa P.RSP.04

Il ripristino delle banche dati tiene conto della loro tipologia come nel caso dell'attivazione del sito Secondario.

Per i file o archivi gestibili tramite gli strumenti di Office Automation vengono ripristinati nelle share di rete secondo la struttura di competenza e le politiche di sicurezza definite nell'ente.

Il ripristino dei Data base vengono eseguiti dai tecnici specializzati della software house fornitrice del software.

3.3.5 Procedura Ripristino delle applicazioni nel sito primario

Procedura Operativa P.RSP.05

Postazioni Client	- Installazione e/o Check di tutto il software necessario all'operatore - Verifica della corretta configurazione degli apparati esterni (scanner, stampanti ecc.) disponibili nella postazione
Server Applicativi	- Installazione e/o Check di tutto il software necessario al ripristino funzionale del sistema - Ripristino dei backup - Verifica di collegamento delle postazioni Client - Verifica della corretta configurazione degli apparati esterni (stampanti ecc.); - Verifica delle procedure di backup/aggiornamento

4 Formazione

La formazione delle risorse riveste un ruolo fondamentale per assicurare la corretta applicazione, conoscenza e padronanza del Piano. Periodicamente è necessario verificare il livello di formazione di tutte le risorse coinvolte nel PCO ICT affinché ciascuna sia ben consapevole delle attività da svolgere in caso di Emergenza. Tutte le risorse coinvolte nel PCO ICT devono essere formate ed istruite circa l'applicazione delle procedure e modalità da seguire nelle diverse attività sia ordinarie sia di emergenza. Il Responsabile della Continuità Operativa ICT assicurare un'efficace pianificazione della formazione sia in termini di periodicità sia di contenuti.

I passi da seguire sono:

- Redazione del piano di formazione
- Redazione del programma di formazione
- Test per la valutazione del livello di conoscenza del Piano
- Relazione di sintesi dei risultati dell'attività formativa

5 Verifica/test del piano

5.1 Obiettivi e strategie di test

Per assicurare una effettiva efficienza nelle operazioni di recovery è prevista l'esecuzione di prove almeno semestrali di funzionalità sia tecnica che organizzativa delle procedure di recovery predisposte. Le prove di recovery coinvolgeranno un sottoinsieme significativo degli utenti del Sistema Informativo, in modo da verificare l'effettiva funzionalità dell'intero processo.

Viene data evidenza dell'esito dei test effettuati in apposite schede, che vengono poi consegnate all'Amministrazione.

5.2 Procedure di test e verifica

La responsabilità dell'esecuzione dei test di continuità operativa è dell'Amministrazione. I tecnici del CBR Asmecloud forniscono assistenza durante queste fasi, secondo quanto opportunamente concordato con l'amministrazione.

La procedura di test e verifica di un evento disastroso e la valutazione della capacità della soluzione proposta di garantire il livello di continuità operativa atteso, in termini tecnologici, organizzativi e procedurali.

Sono possibili numerose modalità di test, eseguite anche contemporaneamente, nel corso di un anno che comprendono almeno: due verifiche teoriche ed una simulazione.

In funzione di esigenze specifiche di organizzazione e/o di cambiamento potranno essere eseguiti ulteriori test.

Si individuano le seguenti tipologie di procedure di test, elencate in ordine crescente di complessità:

- **Verifica teorica:** E' la metodologia più classica, e ricalca le usuali tecniche di auditing e di validazione "su carta". Consiste nel condurre un'analisi di congruenza della soluzione, a cura degli stessi autori della soluzione o di esperti esterni.

- **Verifica strutturata:** Si definisce uno specifico scenario teorico di crisi, e i partecipanti al test operano pedissequamente secondo le modalità previste dal Piano di Continuità operativa. Nel corso della sequenza si verificano e documentano eventuali errori o carenze.
- **Simulazione.** In questo caso il test coinvolge l'intero personale dell'amministrazione o almeno il personale addetto all'area interessata dalla simulazione. Il test prevede l'attivazione "in tempo reale" del piano di continuità operativa e la verifica delle procedure, dei sistemi di backup, dei sistemi alternativi di comunicazione, della mobilitazione dei gruppi di gestione dell'emergenza, del recupero di documenti e dati. Condurre una simulazione di emergenza completa può avere un costo molto elevato; per questo in genere si usano simulazioni semplificate.

Quando sono previsti test periodici di simulazione, valgono i seguenti requisiti:

- le simulazioni devono essere progettate per simulare una "vera" condizione di emergenza, ricreando le conseguenze dell'evento peggiore nel peggior momento tra quelli valutati negli scenari di Risk Assessment (ad esempio, l'improvvisa indisponibilità del Sito Primario durante l'orario di punta dei servizi erogati);
- per non rischiare di compromettere i dati di produzione, per lo svolgimento delle simulazioni, dovranno essere predisposte copie coerenti dei dati ad uso esclusivo della simulazione che saranno cancellate al termine delle prove;
- poiché la soluzione prevede un centro alternativo (nodo secondario del sito secondario), è necessario verificare e testare tutti quei processi e procedure che devono garantire, in condizioni di funzionamento normale del centro primario, le operazioni di allineamento dei due siti.

6 Manutenzione del piano

6.1 Aggiornamento del piano

Il presente piano viene aggiornato entro il 31 dicembre dal Sig. Amato De Rogatis resp. PCO come indicato all'articolo 50 bis del D.lgs 82/2005, il processo e le regole di redazione sono riportate nel seguito:

Le modifiche apportate ad uno qualsiasi dei documenti che costituiscono il Piano, siano essi manuali o allegati esterni, ne comporterà una variazione di modifica e/o release.

Al fine di determinare univocamente la versione/release del Piano, si adotta la seguente metodologia di numerazione:

MAJOR RELEASE . MINOR RELEASE

La modifica di un manuale o di un allegato esterno che scaturisca da una manutenzione ordinaria darà luogo a una nuova minor release del documento (passerà da m.n a m.n+1 ad esempio si passerà dalla release 1.0 alla release 1.1). La modifica di un manuale o di un allegato esterno che scaturisca da una manutenzione straordinaria darà luogo a una nuova major release del documento (passerà da m.n a m+1.0 ad esempio si passerà dalla release 1.5 alla release 2.0).

Dovranno essere aggiornati di conseguenza i dati di controllo presenti nella copertina del documento, la versione nel piè di pagina e la data nell'intestazione.

A ogni nuova versione o release di uno dei documenti che costituiscono il Piano sarà creata una nuova versione o release dell'allegato esterno, tale modifica andrà riportata nella tabella contenuta nel paragrafo 1 "Informazioni Generali" contenente gli estremi delle ultime versioni o release modificate.

La copia cartacea delle nuove versioni o release dovrà essere firmata per approvazione sulla copertina dal responsabile del Gruppo di supporto unitamente alla data di approvazione. Dopo la firma, dovrà essere aggiornata la copia magnetica inserendo il nome del responsabile del Gruppo di supporto e la data di approvazione, e archiviato il documento in formato magnetico/cartaceo secondo lo standard definito.

A ogni nuova versione/release dei documenti che costituiscono il Piano, il Comitato di Gestione della Crisi ha il compito di curare la distribuzione dello stesso affinché le "copie ufficiali" del Piano siano sempre aggiornate.