Allegato delibera
G.C. 17/2016

Piano di Continuita’ Operativa e Disaster Recovery ICT

Comune di Busca

23/07/2014

F I R M E			
	Unità/Ruolo	**Nominativo**	**Firma**
PREPARATO DA:			
CONTROLLATO DA:			
APPROVATO DA:			
AUTORIZZATO DA:			

LISTA DI CONDIVISIONE:

Nominativo	Unità/ Ruolo	Firma

ELENCO DI DISTRIBUZIONE:

Nominativo	Unità

REGISTRO DELLE MODIFICHE		
EDIZIONE	**SINTESI DELLA MODIFICA**	**DATA**

Sommario

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")

1.1 Definizioni e abbreviazioni

Terminologia	Acronimo	Definizione
Piano di Continuità Operativa ICT	PCO ICT	Documento operativo che descrive tutte le attività e modalità finalizzate al ripristino, a seguito di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi classificati come "critici"

Terminologia	Acronimo	Definizione
Piano di Disaster Recovery	PDR	Documento operativo che descrive tutte le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi definiti "critici", il ripristino degli stessi servizi, entro un arco temporale predefinito, tale da rendere, il più possibile, minime le interruzioni nell'erogazione dei servizi. Si evidenzia che il PDR è la sezione del PCO che descrive le attività di ripristino del sistema informativo.

Per ulteriori definizioni di termini ed espressioni che verranno utilizzati, ove non altrimenti specificato, si rimanda al "Glossario" contenuto nelle "Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni".

1.2 Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

- i vertici dell'Amministrazione (Il Sindaco ed il Segretario Comunale);
- il responsabile della CO ICT, così come indicato nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011;
- 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 26 Febbraio 2014 l'Amministrazione ha presentato richiesta di parere, così come previsto dal comma 4 dell'articolo 50-bis del CAD.

In data 15 Maggio 2014 AID ha emesso parere "favorevole condizionato".

1.3.1 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	**RPO**	**RTO**
Albo Pretorio	Media	Tier 3	Tier 3 / Soluzione tecnica unica	4 ore	4 ore
Anagrafe	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
Atti Amministrativi (Delibere e determine)	Media	Tier 2	Tier 3 / Soluzione tecnica unica	3 giorni	3 giorni
Commercio e Polizia Amministrativa	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
Elettorale e Leva	Media	Tier 3	Tier 3 / Soluzione tecnica unica	1 giorno	4 ore
Gestione dei tributi	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
Gestione del bilancio	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	3 giorni
Gestione del personale	Media	Tier 2	Tier 3 / Soluzione tecnica unica	3 giorni	3 giorni
Gestione economato e patrimonio	Media	Tier 2	Tier 3 / Soluzione tecnica unica	3 giorni	3 giorni
Gestione servizi sociali	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	3 giorni
Lavori Pubblici	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	3 giorni
Polizia Locale	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
Protezione Civile	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
Protocollo	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno

Stato Civile e Servizi Cimiteriali	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
SUAP (Sportello Unico Attività Produttive)	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
SUE (Sportello Unico Edilizia)	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
Turismo e Sport	Media	Tier 2	Tier 3 / Soluzione tecnica unica	3 giorni	3 giorni
Ufficio Appalti e Contratti	Media	Tier 2	Tier 3 / Soluzione tecnica unica	3 giorni	3 giorni
Ufficio Cultura	Media	Tier 2	Tier 3 / Soluzione tecnica unica	1 giorno	1 giorno
Urbanistica e Assetto del Territorio	Media	Tier 2	Tier 3 / Soluzione tecnica unica	3 giorni	3 giorni

L'Amministrazione ha ritenuto, invece, non in ambito, i seguenti servizi:

Servizio	Descrizione	Tipologia di utenza
Videosorveglianza	Servizio di controllo degli accessi mediante telecamere	Utente interno
Prenotazione Sale Comunali	Servizio di prenotazione delle sale comunali	Aziende/Cittadini

- ✓ Servizio Videosorveglianza
- ✓ Prenotazione Sale comunali

La videosorveglianza è un servizio altamente specialistico, che utilizza infrastrutture e personale dedicato. Inoltre il servizio non ha dati informatici immagazzinati e storicizzati se non per il tempo strettamente necessario e secondo le normative di legge vigenti e secondo l'apposito regolamento comunale.

La prenotazione delle Sale comunali è un servizio accessorio non strettamente indispensabile.

Si è altresì proceduto, come da richiesta allegata al parere a produrre l'analisi delle valutazioni di criticità dei servizi fuori ambito che di seguito riassumiamo:

Servizio / classe servizi	Classe criticità	Sol. tecnologica minima da autovalutazione	Soluzione **tecnica** individuata	**RPO**	**RTO**
Videosorveglianza	Media	Tier 2	Fuori ambito	1 giorno	1 giorno
Prenotazione sale comunali	Bassa	Tier 1	Fuori ambito	1 settimana	1 settimana

1.3.2 La sintesi del parere di AID.

In data 15 Maggio 2014 AID ha emesso parere “favorevole condizionato” con le seguenti osservazioni:

1) L’Amministrazione verifichi presso la propria Regione, prima di dare avvio alle Soluzioni, la presenza di piani regionali conseguenti a questo disposto dall’art 33-septies del D.L. 179 convertito nella legge 221/2012;

2) L’Amministrazione relativamente ai servizi non in ambito, entro e non oltre dieci giorni dall’emissione del presente fornisca:

    - Valutazione criticità degli stessi;

3) Relativamente alla soluzione tecnica, 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;

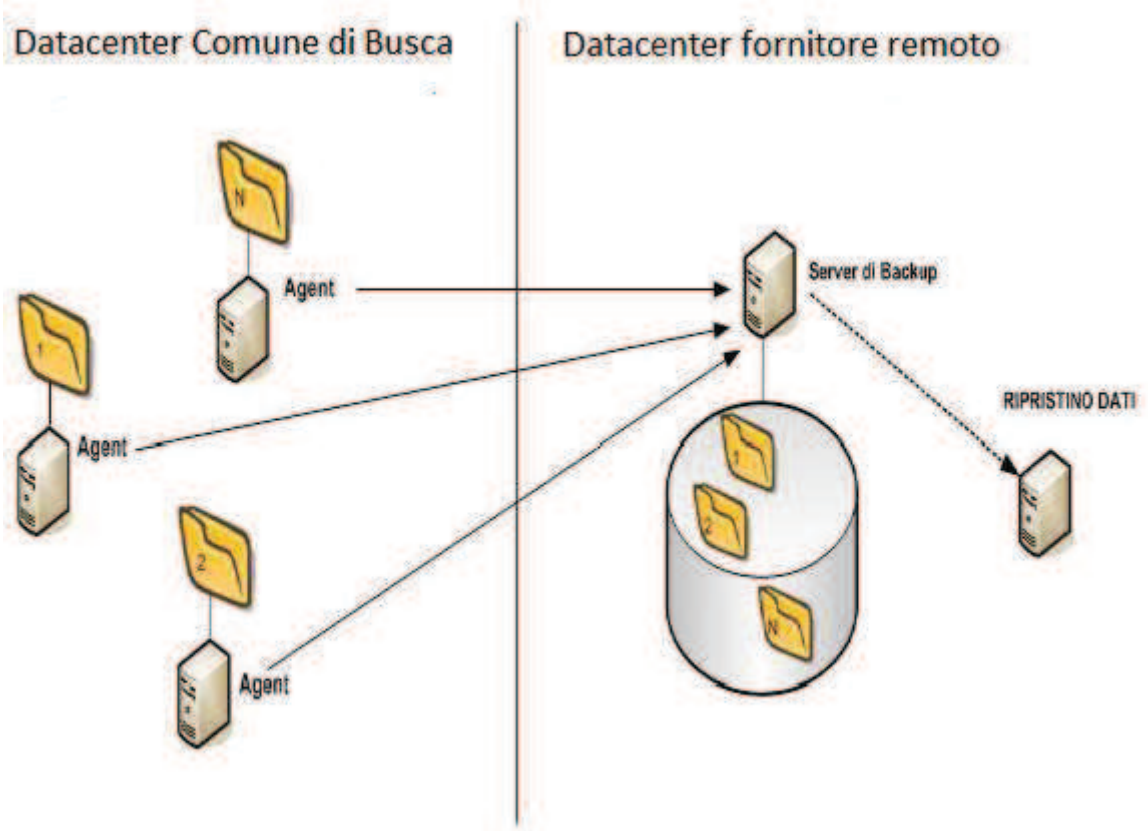
4) La soluzione tecnica di continuità operativa sia coerente con i requisiti definiti in fase di autovalutazione e vengano verificati i requisiti sopra indicati della soluzione stessa;

5) venga verificato, nell’implementazione della soluzione tecnica di DR descritta, 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);

6) relativamente al coinvolgimento di fornitori esterni per l’implementazione della soluzione tecnica individuata dall’Amministrazione, si richiama quest’ultima alla verifica di questa scelta sotto il profilo della normativa vigente (Dlgs 12 aprile 2006 n. 163 e s.m.i. e DPR207/2010).

1.3.3 Variazioni eventuali nel numero dei servizi e relative criticità.

Relativamente alla soluzione tecnica, tenendo in conto quanto indicato ai punti 1 e 3 delle osservazioni relative all'approvazione dello studio di fattibilità, e tenendo conto delle difficoltà relative al reperire le risorse economiche, è stato deciso di mantenere l'attuale soluzione tecnica di DR in grado di garantire il livello tecnologico (TIER) approvato dallo studio di fattibilità. La soluzione è quella del Cloud Backup dove vengono trasferite delle copie di sicurezza dei propri dati nel luogo sicuro del sito secondario (sito di replica), al fine di garantire la conservazione dei dati vitali a fronte a qualsiasi evenienza disastrosa. Tramite un'unica console di gestione centralizzata, è possibile automatizzare la protezione globale e i criteri di conservazione, mentre un accesso sicuro, self-service aumenta la disponibilità delle informazioni e diminuisce i tempi necessari all'accesso dei dati.
Tale schema di conservazione dei dati è riassunto nello schema:



Tale soluzione ricomprende tutti i servizi descritti nel perimetro dello studio di fattibilità come sotto elencato:

Servizio / classe servizi	Classe criticità	Sol. tecnologica minima da autovalutazione	Soluzione **tecnica** individuata	**Variazioni**
Atti Amministrativi	Media	Tier 3	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Tributi	Bassa	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Gestione Finanziaria	Media	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Gestione Polizia Municipale	Media	Tier 3	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Protocollo	Media	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Gestione Casa di Riposo Comunale	Media	Tier 3	Tier 3 / Soluzione tecnica unica	Nessuna variazione
SUAP	Bassa	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Edilizia Privata	Bassa	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Urbanistica e Lavori Pubblici	Bassa	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Servizi Cimiteriali	Media	Tier 3	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Personale	Media	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Servizi Demografici	Media	Tier 3	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Stipendi	Media	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Albo Pretorio	Media	Tier 2	Tier 3 / Soluzione tecnica unica	Nessuna variazione
Protezione Civile	Media	Tier 3	Tier 3 / Soluzione tecnica unica	Nessuna variazione

La soluzione della soluzione di Continuità Operativa adottata dal Comune di Busca è gestita dal fornitore A. & C. Servizi / Kelyan s.p.a. ed è stata implementata a partire dall'agosto 2013.

1.4 Sintesi di informazioni organizzative e tecniche sull'Amministrazione

1.4.1 Matrice servizi/organizzazione (responsabilità)

SERVIZIO	UFFICIO RESPONSABILE	RESPONSABILE
Albo Pretorio	Polizia Locale	Acchiardi Gianluca
Anagrafe	Demografico	Armando Silvio
Atti Amministrativi (Delibere e determine)	Segretario Comunale	Scarpello Giusto
Commercio e Polizia Amministrativa	Polizia Locale	Acchiardi Gianluca
Elettorale e Leva	Demografico	Armando Silvio
Gestione dei tributi	Ragioneria – Tributi	Rotolone Ivano
Gestione del bilancio	Ragioneria – Tributi	Rotolone Ivano
Gestione del personale	Segretario Comunale	Scarpello Giusto
Gestione economato e patrimonio	Ragioneria – Tributi (economato) Ufficio Tecnico E.P. (patrimonio)	Rotolone Ivano Gosso Pier Luigi
Gestione servizi sociali	Segreteria	Armando Silvio
Lavori Pubblici	Ufficio Tecnico LL.PP.	Tallone Bruno
Polizia Locale	Polizia Locale	Acchiardi Gianluca
Protezione Civile	Polizia Locale	Acchiardi Gianluca
Protocollo	Segreteria	Armando Silvio
Stato Civile e Servizi Cimiteriali	Demografico	Armando Silvio
SUAP (Sportello Unico Attività Produttive)	Ufficio Tecnico E.P.	Gosso Pier Luigi
SUE (Sportello Unico Edilizia)	Ufficio Tecnico E.P.	Gosso Pier Luigi
Turismo e Sport	Segretario Comunale (turismo) Ufficio Tecnico E.P. (Sport)	Scarpello Giusto Gosso Pier Luigi
Ufficio Appalti e Contratti	Segreteria	Armando Silvio
Ufficio Cultura	Segreteria	Armando Silvio
Urbanistica e Assetto del Territorio	Ufficio Tecnico E.P.	Gosso Pier Luigi

1.4.2 Matrice servizi/infrastruttura tecnologica

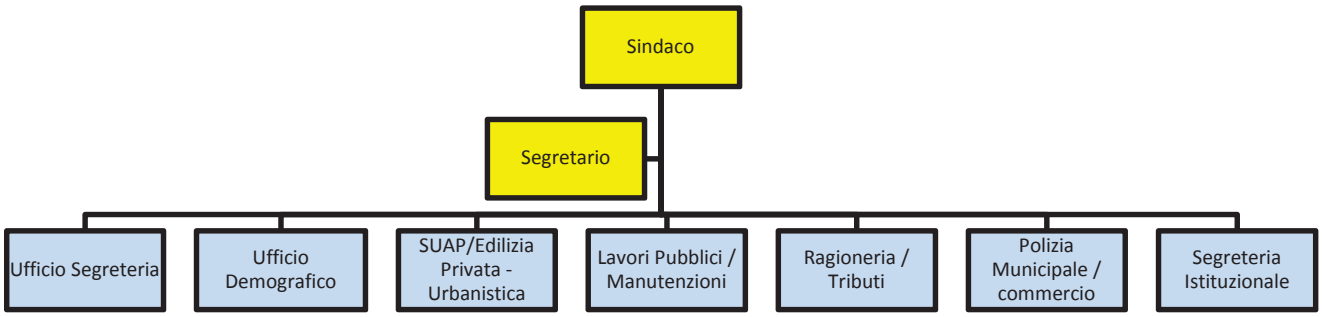
SERVIZIO	SISTEMA (I) DI ESERCIZIO	LOCALIZZAZIONE	LDS (orario disponibilità)
Albo Pretorio	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale.	24 ore giornaliere
Anagrafe	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Atti Amministrativi (Delibere e determine)	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	8 ore giornaliere
Commercio e Polizia Amministrativa	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Elettorale e Leva	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Gestione dei tributi	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Gestione del bilancio	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	8 ore giornaliere
Gestione del personale	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	8 ore giornaliere
Gestione economato e patrimonio	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	8 ore giornaliere
Gestione servizi sociali	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Lavori Pubblici	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	8 ore giornaliere
Polizia Locale	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	12 ore giornaliere
Protezione Civile	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	12 ore giornaliere
Protocollo	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Stato Civile e Servizi Cimiteriali	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	8 ore giornaliere
SUAP (Sportello Unico Attività	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
SUE (Sportello Unico Edilizia)	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Turismo e Sport	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Ufficio Appalti e Contratti	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Ufficio Cultura	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere
Urbanistica e Assetto del Territorio	Ced Server	Server Comunale dislocato presso la sala server Municipale situato al primo piano del palazzo comunale	Fino a 6 ore giornaliere

2 Predisposizione all'emergenza

2.1 La struttura organizzativa

Coerentemente con la normativa vigente, vale a dire il testo unico delle autonomie locali (TUEL) del 2000 (decreto legislativo 267/2000), il Comune esercita tutte le funzioni amministrative che riguardano la popolazione ed il territorio comunale, precipuamente nei settori organici dei servizi alla persona e alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico, salvo quanto non sia espressamente attribuito ad altri soggetti dalla legge statale o regionale, secondo le rispettive competenze.

L'Ente espleta le proprie funzioni istituzionali mediante la seguente struttura organizzativa:



2.2 Comitato di crisi ICT

TABELLA INDIRIZZI E-MAIL DEL COMITATO DI GESTIONE CRISI

NOME E COGNOME	RUOLO	POSTA ELETTRONICA
Silvio Armando	Responsabile della Continuità Operativa	silvioarmando@comune.busca.cn.it
Marco Gallo	Sindaco	sindaco@comune.busca.cn.it
Giusto Scarpello	Segretario Comunale	segretario@comune.busca.cn.it
Bruno Tallone	Responsabile sicurezza e manutenzioni	brunotallone@comune.busca.cn.it
A&C Servizi	Responsabile manutenzione esterna	

Ruoli necessari:

- Il Sindaco e il Segretario Comunale;
- Il Responsabile della "continuità operativa" dell'ente
- Il Responsabile dell'Unità locale di sicurezza prevista dal DPCM 01.04.2008
- I referenti tecnici (anche presso i fornitori di servizi ICT) di volta in volta necessari alla gestione della crisi
- Il Responsabile della logistica
- Il Responsabile della safety dell'ente
- Il Responsabile delle applicazioni
- I Responsabili di settore

2.3 Responsabile della Continuità Operativa ICT

Svolge le funzioni di Responsabile della Continuità operative il dott. **Silvio Armando** vice segretario comunale.

2.4 Strutture tecniche

SITO PRIMARIO

Il sito primario è ubicato nel palazzo comunale al primo piano sito in via Cavour al civico 28 esteso su due piani oltre al pano terreno. Al piano terreno sono siti gli uffici relativi ai tributi e polizia locale, al primo piano sono dislocati la sala del server, ufficio del segretario comunale, segreteria, Demografici e Ragioneria. Al secondo piano, infine, sono ubicati gli uffici Tecnico. L'ubicazione della sala server e degli uffici è comunque conoscibile dalle piantina allegata nell'Allegato A. La rete informatica è descritta nello schema presente nell'Allegato B. La connessione del sito primario è gestita dal fornitore Mareneonline tramite rete cablata e Hyperlan.

SITO SECONDARIO (SITO DI REPLICA)

Il sito secondario (Sito di replica) è ubicato nella città di Rozzano Milanese in viale Toscana numero 23 presso la sede della server farm della Telecom Italia.

Le caratteristiche principali del sito secondario di replica (server farm Telecom Italia) sono:

- disponibilità Globale dei Sistemi: 99,9%
- massimi standard di sicurezza fisica e logica
- gestione Operativa e Sistemistica 24h/7gg
- help desk basato su personale specializzato, strumenti di monitoraggio e gestione dei disservizi, con servizio di Customer Care all'avanguardia funzionale 24h/7gg, 365 gg all'anno.

La sicurezza fisica del sito è garantita da avanzati sistemi e procedure che garantiscono al meglio la qualità del servizio offerto nel dettaglio:

- rivelazione fumi e spegnimento incendi
- sistemi anti allagamento e anti intrusione
- sistemi di condizionamento, continuità ed emergenza
- controllo degli accessi fisici all'IDC e telecamere a circuito chiuso

E' possibile ottenere anche l'accesso fisico presso la struttura del sito secondario di replica aprendo un ticket con il fornitore Kelyan (A&C Servizi) indicando i dati della carta di identità della persona incaricata all'ingresso nella struttura. Tempi necessari per l'apertura del ticket sono stimabili in 4 ore.

Possibili sito utilizzabile per la ripartenza dei servizi, qualora siano agibili nel caso di evento distruttivo di tipo non esteso, è nel Comune di Busca:

1. Scuola elementari di Busca concentrico site in via C. Michelis n° 2 (Telefono 0171/945128) che dispone di locali adeguati e di collegamento alla rete internet. La struttura dispone altresì di impianto. L'accesso alla struttura e possibile senza necessità di chiavi in orario di apertura.

I locali delle scuole elementari di Busca concentrico sono a norma dal punto di vista dell'impianto elettrico e antincendio e nei locali attualmente adibiti a segreteria della scuola siti al piano terreno della struttura è presente la connessione a internet ed una rete informatica con diverse postazioni informatiche.

Nel caso di eventi distribuiti sul territorio e/o di inagibilità delle strutture alternative proposte e nell'eventualità di mancanza di materiale informatico è possibile acquisire sul mercato con procedura di acquisto in emergenza gestite dal Comitato di gestione della Crisi il materiale/l'utilizzo delle strutture.

In tale situazione assumerà la massima importanza la verifica con la Regione Piemonte di quanto disposto dall'eventuale **piano regionale** conseguente a quanto disposto dall'articolo 33-septies del D.L. 179 convertito nella legge 221/2012 (consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del paese).

La scelta del sito alternativo non deve prescindere dalla verifica puntuale delle caratteristiche del sito che dovranno rispettare le caratteristiche minime essenziali come definite dal documento dell'AGID "I servizi minimi essenziali per l'adozione delle soluzioni di disaster recovery" relativamente al servizio "**D3 – Sito di Disaster Recovery: aree CED e aree attrezzate per i posti di lavoro**" .

2.5 Composizione, ruoli, procedure operative

I soggetti coinvolti sono i seguenti:

UFFICIO	RUOLO	DESCRIZIONE RUOLO	FIGURA PROFESSIONALE	RESPONSABILITA'
UFFICIO SEGRETERIA	Responsabile dei sistemi informativi	Coordina e verifica la struttura tecnica legata alla gestione delle informazioni, alla corretta configurazione e gestione dell'hardware	Dirigente/Istruttore Direttivo	Reponsabile dell'attuazione del piano di DR
SEGRETARIO COMUNALE	Segretario Comunale	Coordina i Responsabili di Settore o Area	Segretario Comunale	Coordina i Responsabili di servizio e impartisce idonei obiettivi per la gestione della Crisi
UFFICIO SERVIZI FINANZIARI	Responsabile / dirigente di settore	Gestione delle risorse finanziarie per fronteggiare la crisi e rientrare dall'emergenza	Dirigente/Istruttore Direttivo	Responsabilità: adeguare le disponibilità di bilancio per far fronte agli oneri della Continuità Operativa ICT
TECNICI A&C SERVIZI / KELYAN	Tecnici qualificati presso A&C servizi / Kelyan	Coordinamento delle procedure di Disaster Recovery .	Tecnico	Coadiuvanti nelle procedure di gestione del sito secondario dall'attivazione al rientro

2.6 Gestione delle reperibilità

Il Piano di Continuità Operativa comunale prevede che in caso di annuncio di condizioni di emergenza, l'istituto della reperibilità sia estesa in una prima fase a tutti i dipenti richiamati dal precedente paragrafo e anche , su disposizione del Comitato di Crisi, in fase successiva esteso a tutti i dipendenti e/o collaboratori che dovessero essere ritenuti necessari.

Per quanto riguarda le forniture di servizi esterni ICT richieste dal momento di necessità viene prevista una integrazione contrattuale con la quale si dispongono termini e condizioni dell'intervento per la gestione delle situazioni d'emergenza.

3 Soluzione di continuità

La soluzione di continuità operativa è la medesima per tutti i servizi gestiti in ambito comunale e definiti in ambito come da schema definito nel paragrafo 1.3.3 che ovviamente non comprende i servizi non in ambito che restano esterni al perimetro della Continuità Operativa.

Come sopra spiegato in questa fase si è deciso di mantenere l'attuale soluzione tecnica di DR in grado di garantire il livello tecnologico (TIER) approvato dallo studio di fattibilità. La soluzione è quella del Cloud Backup dove vengono trasferite delle copie di sicurezza dei propri dati nel luogo sicuro del sito secondario (sito di replica), al fine di garantire la conservazione dei dati vitali a fronte a qualsiasi evenienza disastrosa. Tramite un'unica console di gestione centralizzata, è possibile automatizzare la protezione globale e i criteri di conservazione, mentre un accesso sicuro, self-service aumenta la disponibilità delle informazioni e diminuisce i tempi necessari all'accesso dei dati.

Servizi ricompresi nella soluzione di continuità operativa

Servizio / classe servizi	Classe criticità	Sol. tecnologica minima da autovalutazione	**Variazioni**
Albo Pretorio	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
Anagrafe	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Atti Amministrativi (Delibere e determine)	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Commercio e Polizia Amministrativa	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
Elettorale e Leva	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Gestione dei tributi	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
Gestione del bilancio	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Gestione del personale	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Gestione economato e patrimonio	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Gestione servizi sociali	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
Lavori Pubblici	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup

Polizia Locale	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
Protezione Civile	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Protocollo	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Stato Civile e Servizi Cimiteriali	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
SUAP (Sportello Unico Attività Produttive)	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
SUE (Sportello Unico Edilizia)	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Turismo e Sport	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Ufficio Appalti e Contratti	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup
Ufficio Cultura	Media	Tier 2	Nessuna variazione: Attuazione del Cloud backup
Urbanistica e Assetto del Territorio	Media	Tier 3	Nessuna variazione: Attuazione del Cloud backup

3.1 Interrelazioni del servizio/i con entità esterne all'Amministrazione

ENTITA'	Applicativo Utilizzato/supporti utilizzati	DIREZIONE FLUSSI/FORNITORE
Albo Pretorio	Saturn	Gestione dell'applicativo fornito dalla SISCOM SPA.
Anagrafe	Selene	Gestione dell'applicativo fornito dalla SISCOM SPA.
Atti Amministrativi (Delibere e determine)	Venere	Gestione dell'applicativo fornito dalla SISCOM SPA.
Commercio e Polizia Amministrativa		
Elettorale e Leva	Selene	Gestione dell'applicativo fornito dalla SISCOM SPA.
Gestione dei tributi	Piranha	Gestione dell'applicativo fornito dalla SISCOM SPA.
Gestione del bilancio	Giove	Gestione dell'applicativo fornito dalla SISCOM SPA.
Gestione del personale		

Gestione economato e patrimonio	Io	Gestione dell'applicativo fornito dalla SISCOM SPA
Gestione servizi sociali		
Lavori Pubblici		
Polizia Locale	Urano	Gestione dell'applicativo fornito dalla SISCOM SPA
Protezione Civile		
Protocollo	Egisto	Gestione dell'applicativo fornito dalla SISCOM SPA
Stato Civile e Servizi Cimiteriali	Sesamo	Gestione dell'applicativo fornito dalla SISCOM SPA
SUAP (Sportello Unico Attività Produttive)	Gismaster SUAP	Gestione dell'applicativo fornito dalla TECNICAL DESIGN
SUE (Sportello Unico Edilizia)		
Turismo e Sport		
Ufficio Appalti e Contratti	Venereco	Gestione dell'applicativo fornito dalla SISCOM SPA
Ufficio Cultura		
Urbanistica e Assetto del Territorio		

3.2 Dati logistici generali

Il punto di ritrovo principale è il Municipio sito in Via Camillo Benso conte di Cavour al civico numero 28.

La sede secondaria, in caso di impossibilità di accesso, agibilità e utilizzo dei locali della sede primaria è ubicata presso la sede delle Scuole Elementari Busca concentrico site in via C. Michelis, 2 (Telefono 0171/945128) che dispone di locale adeguatio e di connessione alla rete internet.

La struttura dispone altresì di impianto antincendio e di rilevatore di fumi oltre che di impianto elettrico e di riscaldamento a norma che permetterebbero la possibiltà di un rapido ripristino delle funzionalità comunali. L'accesso è autorizzato senza necessità di chiavi.

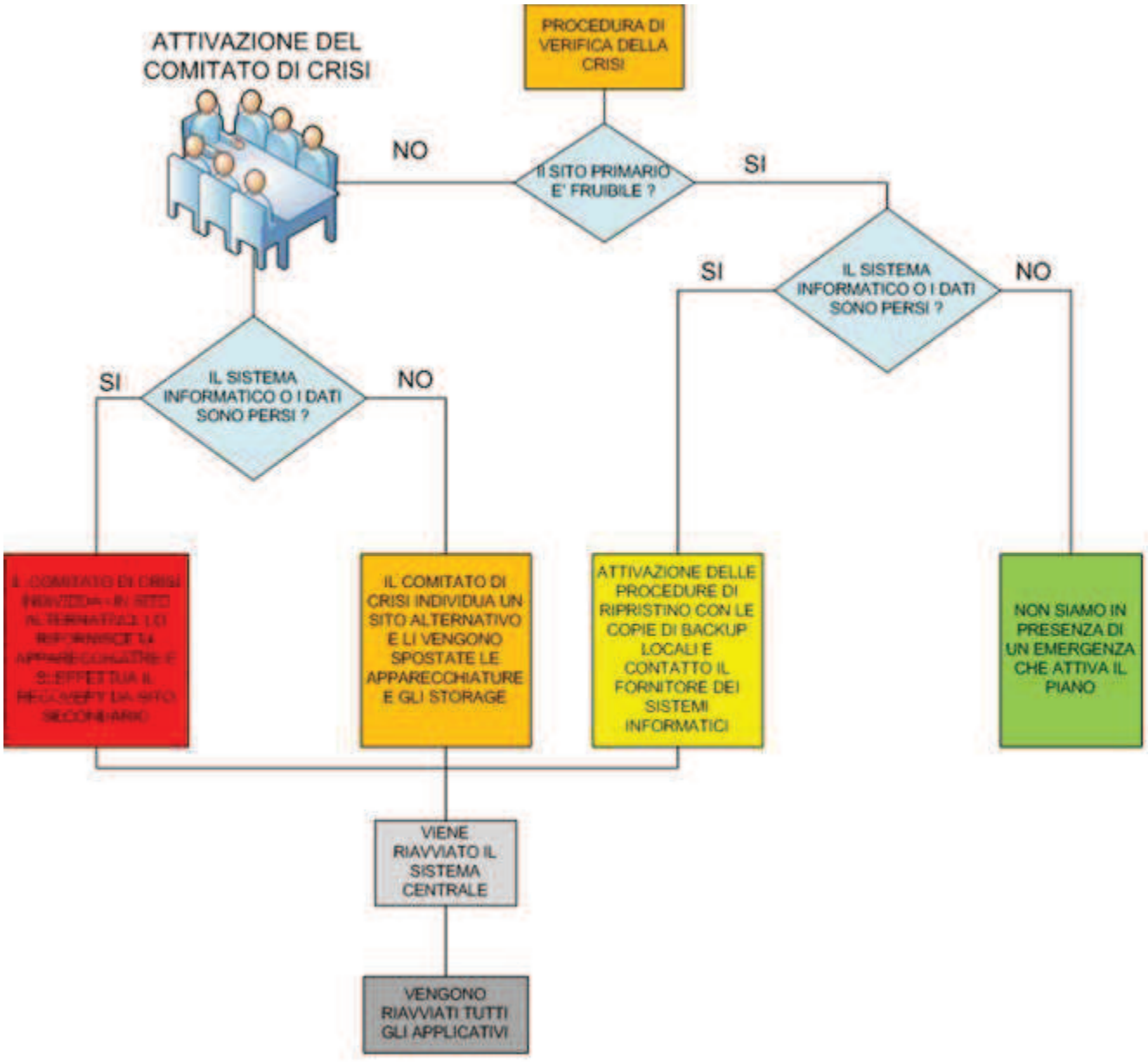
Nel caso non sia possibile operare presso il sito primario di produzione dei dati, il Comitato di Gestione Crisi dichiarerà lo spostamento del personale e delle infrastrutture trasportabili, e darà dettaglio delle modalità di spostamento a seconda della gravità dei casi di disastro tenendo conto che nel caso il sito secondario proposto non sia utilizzabile sarà possibile identificare altri siti attingendo alle modalità di emergenza per l'individuazione di un sito alternativo.

3.3 Scenari di emergenza applicabili

La soluzione tecnologica come stabilito in fase di Studio di Fattibilità è di TIER 3 è scelto dovrebbe garantire di rispettare i tempi di RPO e di RPO dichiarati in fase di Studio di Fattibilità Tecnica (come da tabella 1.3.1. per tutti i servizi considerati).

3.4 Fase di reazione all'emergenza

3.15.1 Processo preliminare di attivazione dell'emergenza



In caso di eventi che colpiscono la sede comunale ogni Responsabile/Referente di Area è tenuto ad utilizzare la seguente tabella per determinare il grado di severità dell'incidente ed eventualmente notificare al Responsabile della Continuità operativa o suo delegato l'evento incidentale se ritenuto di categoria "Grave" o "Disastroso", come meglio descritto nella seguente tabella relativa alla classificazione degli incidenti con i livelli di disastro.

LIVELLO	CLASSE INCIDENTE	DESCRIZIONE	RESPONSABILITA'
1	**ORDINARIO**	L'incidente non provoca disservizi importanti e l'impatto sull'operatività dell'Ente non è rilevante. L'evento è risolvibile con mezzi d'intervento ordinari.	Responsabile di Area/Servizio o suo delegato
2	**SIGNIFICATIVO**	Degrado o interruzione di servizi non critici per cui non vengono interessate nel disservizio un numero elevato di persone/utenti. L'incidente potrebbe provocare l'arresto di uno o più servizi senza però pregiudicare la continuità operativa dell'Ente in quanto il problema può essere risolto con l'utilizzo di mezzi di intervento/risorse ordinarie.	Responsabile di Area/Servizio o suo delegato
3	**GRAVE**	Interruzione dei servizi più importanti/critici che potrebbero compromettere la continuità operativa dell'Ente o che creano un disservizio che coinvolge un numero elevato di persone. Valutazione dell'incidente in termini di mezzi di intervento in quanto potrebbe non essere risolvibile velocemente e potrebbe essere necessaria l'attivazione di risorse elevate e/o non valutabili.	A discrezione del Responsabile della Continuità Operativa
4	**DISASTROSO**	Incidente che causa l'interruzione dei servizi per un periodo superiore a quanto indicato nella tabella 1.3.1. senza la possibilità di intervenire con trattazioni alternative.	Comitato di Gestione Crisi

Il **Responsabile della Continuità Operativa**, ha il compito di contattare tutte le figure del Comitato di Gestione Crisi per le riunione periodiche e provvedere agli aggiornamenti dei piani. Provvede, inoltre, ad avvisare le figure del Comitato di Gestione Crisi almeno 15 giorni prima della data fissata tramite posta elettronica, nel seguito sarà riportata la tabella con gli indirizzi mail delle persone interessate.
Sarà suo compito valutare se l'evento seganalato è tale da generare una possibile situazione di emergenza e, quindi coinvolgere il Comitato di crisi ICT, oppure se l'evento va gestito con le "normali" procedure di gestione degli incidenti.
In caso di dichiarazione disastro/emergenza il RCO provvede a contattare tutte le figure facenti parte del Comitato di Gestione Crisi secondo i riferimenti presenti nel paragrafo 2.2.1.
In caso di dichiarazione di disastro/emergenza il RCO provvede inoltre a redigere una relazione che illustri le fasi e l'evoluzione dell'emergenza e, una volta rientrata, dovrà essere inviata all'Agenzia per l'Italia Digitale.

Il Comitato di Gestione Crisi è l'organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività delle risorse coinvolte nel piano di Continuità Operativa e di Disaster Recovery; è l'organo di direzione strategica dell'intera struttura in occasione dell'apertura della crisi e, inoltre, ha la responsabilità di garanzia e controllo sull'intero progetto.
Le figure minime necessarie per la costituzione del Comitato di gestione della crisi sono rappresentate da:

- Un ruolo di vertice con poteri decisionali e di indirizzo in materia organizzativa ed economica, ovvero il responsabile dell'Ufficio Unico Dirigenziale ex art. 17 del CAD;
- Il Responsabile della "Continuità Operativa" dell'ente;
- Il Responsabile dell'Unità locale di sicurezza prevista dal DPCM 01.04.2008;
- I referenti tecnici (anche presso i fornitori di servizi ICT) di volta in volta necessari alla gestione della crisi;
- Il responsabile della logistica;
- Il responsabile della safety dell'ente;
- Il responsabile delle applicazioni.

Le procedure di acquisto in emergenza sono attivabili secondo quanto indicato dal regolamento interno dell'Ente. Tutti gli acquisti vanno valutati in sede di gestione del Comitato di crisi.

I compiti isituzionali del Comitato di crisi sono:

- Definizione ed approvazione del piano di continuità operativa;
- Valutazione delle situazioni 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;
- Avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
- Dichiarazione di rientro.

In condizioni di incidente **disastroso**, il Comitato assume il controllo di tutte le operazioni e assume le responsabilità sulle decisioni per affrontare l'emergenza, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.
In condizioni di incidente grave, il Responsabile della Continuità Operativa può decidere di lasciare il coordinamento delle operazioni al Responsabile di Area coinvolto, oppure al Comitato di Crisi stesso.

Per svolgere i propri compiti, il Comitato attiva le altre figure identificate come risorse dell'Unità Locale di Sicurezza, che fa in modo che il Comitato possa disporre di strumenti e competenze per affrontare ogni sua decisione.

Il Comitato deve in caso di **decretazione dell'inagibilità completa o parziale di alcune aree dell'ente** provvedere a:

- Individuare un sito alternativo
- Predisporre un collegamento di rete (connessione dati) con il sito Primario (se ancora fruibile) e con il sito Secondario
- Individuazione del nucleo iniziale di incaricati necessari per fronteggiare la crisi
- Dotare di postazioni informatiche adeguate, al collegamento di rete (connessione dati) un nucleo di persone individuate come incaricati per fronteggiare la crisi.
- Decidere se andare ad aumentare il numero di postazioni informatiche di base individuate per la partenza della gestione della crisi in funzione delle esigenze e degli scenari che si andranno a presentare.

Il Comitato deve essere supportato nelle seguenti aree:

- Area logistica, per garantire supporto negli eventuali spostamenti;
- Area tecnologica, per garantire il funzionamento e l'accesso a tutte le infrastrutture informatiche e di telecomunicazioni predisposte;
- Area informazioni, per aggiornare il Comitato relativamente alle notizie provenienti dai canali pubblici di comunicazione;
- Area comunicazioni di processo, per provvedere alla raccolta di tutta la documentazione dai vari gruppi di lavoro.

Può essere necessario assicurare al Comitato un supporto anche sulle aree:

- Comunicazioni, ad esempio tramite valutazione delle strategie di comunicazione verso cittadini, organizzazioni e dipendenti e dei canali da utilizzare per ciascun tipo di comunicato;
- Finanza, ad esempio con definizione di tutte le iniziative di carattere finanziario necessarie ad assicurare risorse tempestive;
- Risorse umane e rapporti sindacali, ad esempio definizione di comportamenti e formulazione di messaggi specifici volti a rassicurare i dipendenti, sensibilizzare quelli coinvolti nelle operazioni di ripristino, dirimere ogni possibile motivo di disagio che possa ridurre l'efficacia dell'organizzazione;
- Sicurezza informatica, con l'esame di tutti gli aspetti di sicurezza, in particolare per quanto riguarda la verifica del grado di sicurezza offerto dalle configurazioni adottate per l'emergenza e la protezione dei dati, o tramite il riesame delle soluzioni adottate per il

ripristino dei sistemi e per il rientro alla normalità;

- Area legale, per eventuali azioni nei confronti del fornitore della soluzione di CO (es. per il mancato rispetto dei tempi di RTO/RPO).

Le date delle riunioni del Comitato saranno decise di volta in volta nel corso della riunione precedente e ne sarà dato atto in appositi verbali sottoscritti e depositati presso gli uffici del Comune. Si precisa inoltre che la validità delle soluzioni e delle azioni presenti nel Piano di Continuità Operativa e nel Piano di Disaster Recovery saranno valutate annualmente e ne verrà dato atto nei verbali delle riunioni del Comitato di Gestione Crisi.

3.5 Fase di gestione dell'emergenza e riattivazione dei servizi

La fase di gestione dell'emergenza e riattivazione dei servizi fase è ripartita in due sottofasi:

- Ripristino fisico dell'Hardware e del software necessario al funzionamento dell'infrastruttura
- Ripristino delle banche dati

3.16.1 Ripristino fisico dell'Hardware e del software necessario al funzionamento dell'infrastruttura

Attivato il sito alternativo, utilizzando dove possibile il materiale proveniente dal sito Primario integrato con le macchine eventualmente presenti (nel sito scuole elementari Busca concentrico possono essere presenti macchine utilizzabili) o attivando le procedure di acquisto in emergenza gestite dal Comitato di gestione della Crisi, è necessario procedere con l'avvio (start-up) dei sistemi al fine di ripristinare i servizi dell'Ente.

Il Comune di Busca dispone di contratti di assistenza con le ditte Marene Online snc, Siscom, AeC Servizi, Technical Design che assicurano un tempo di intervento minimo dopo la richiesta di intervento con presenza in loco dei propri tecnici se necessaria. Per quanto riguarda la ditta Marene Online snc si allega la lettera di rassicurazione ottenuta in tal senso che è contenuta nell'Allegato C.

La fase di "virtualizzazione" delle macchine dell'Ente è **completa** pertanto, per il ripristino delle funzionalità non dovranno essere reinstallati sistemi operativi e /o applicativi specifici (questo rappresenta una velocizzazione dei processi necessari al ripristino della Continuità Operativa).

La "virtualizzazione" dei Server, infatti, permette di intraprendere una politica di Disaster Recovery molto più efficace. Utilizzando Server virtuali, questi ultimi possono essere ospitati su un'unica macchina per quanto riguarda l'hardware, con ambiente operativo, che funge da base per l'installazione e la gestione dei Server installati virtualmente.
Le "virtual machine" non hanno un legame diretto con l'hardware della macchina per quanto riguarda i

driver, ma utilizzano dei driver generici che si interfacciano a periferiche virtuali. Questa circostanza fa si che la macchina virtuale possa essere gestita come un semplice software. L'immagine del Server Virtuale può essere esportata e ripristinata su qualsiasi altra macchina proprio in quanto slegata dalla apparecchiatura ospitante. In sostanza un Server fisico può ospitare più Server virtuali e, cosa fondamentale, possono essere salvati come immagine e ripristinati sulla stessa o su altre macchine, dette anche di fortuna, senza perdere funzionalità ovvero dati e senza necessità di interventi tecnici particolarmente complessi.

La prima fase, sul sito alternativo, dovrà essere quella di effettuare il riavvio delle macchine disponibili assicurando la funzionalità **del 40% delle postazioni presenti nel sito primario** sulle quali dovranno essere resi disponibili gli applicativi necessari al funzionamento dei servizi.

I responsabili tecnici dell'ente hanno il compito di gestire autonomamente e/o con il supporto dei tecnici dei fornitori esterni elencati nel capitolo 3.1 l'installazione e la configurazione degli specifici applicativi di pertinenza delle varie aree dell'Ente presenti sul Server centrale e sulle postazioni client testando anche il funzionamento degli applicativi e seganalando/risolvendo in autonomo eventuali problematiche.

3.16.2 Ripristino delle banche dati

Il ripristino delle banche dati deve essere fatto qualora siano utilizzabili/recuperabili attingendo nell'ordine dalle seguenti fonti:

1. Server del sito Primario
2. Backup locali del sito Primario
3. Cloud Backup del sito Secondario

La scelta definitiva deve essere fatta ascoltando l'analisi tecnica fornita rispetto allo stato di fatto dell'integrità delle banche dati disponibili sulla base dell'evento disastroso che ha colpito l'ente è spetta al comitato di crisi.

Nel caso si utilizzino una delle prime due casisitiche la disponibilità dei dati è immediata essendo questi presenti direttamente già all'interno della sede alternativa; nel caso invece si utilizzi la terza procedura dovrà essere valutato se i tempi di **trasferimento dei dati** sulla base della connessione che sarà a disposizione del sito alternativo sia compatibile sulla base della quantità di dati che si devono spostare dal sito secondario al sito alternativo a quello primario per mettere a disposizione i backup. Qualora le tempistiche risultino non adeguate sarà possibile concordare con il fornitore del servizio di cloud backup la fornitura di dati su supporti alternativi.

Vengono di seguito riportate le procedure di ripristino relative ai punti 2 e 3 dell'elenco sopra indicato.

3.16.3 Modalità di ripristino dati tramite backup locale del Sito Primario

Il sito primario dispone di un sistema di backup che permette di duplicare tutti i dati trattati anche relativi alle banche dati che attualmente non fanno parte servizi gestiti in ambito, è presente fisicamente e pertanto è da considerare come fonte primaria dei dati a cui attingere nel momento in cui si renda necessario un ripristino dei dati e la copia risulti ancora disponibile.

Il sistema di backup dei dati consiste, come da schema allegato, in due Nas che sono la perfetta copia dei dati presenti sul disco primario dei server e da cassetta dds4 che viene replicata giornalmente, mensilmente e annualmente gestito in automatico dal software bckup exec della Symantec.

Per il ripristino dei dati necessario fare accesso ai Nas o ai supporti cassetta necessari e accedere direttamente ai file necessari alla ripartenza dei servizi. In ogni momento è possibile richiedere l'intervento dei servizi esterni /aziende fornitrici interessate al processo di cui al capitolo 2.2.1.

3.16.4 Modalità di ripristino dati tramite cloud backup dal Sito Secondario

Il ripristino consente di recuperare file/directory archiviati dal servizio secondo la ritenzione richiesta e il calendario di backup impostato accedendo al sito *https://saferecovery.netteam.it* con le credenziali (Nome Utente e Password) conservate dal Responsabile della Continuità Operativa.

In alternativa con un operazione più veloce, sempre che l'unità locale non sia compromessa, è possibile accedere al backup locale tramite sito *http://ctera-c200/* con le credenziali (Nome Utente e Password) anche in questo caso conservate dal Responsabile della Continuità Operativa.

Andremo di seguito ad esplicare le due modalità distinte di ripristino dei dati.

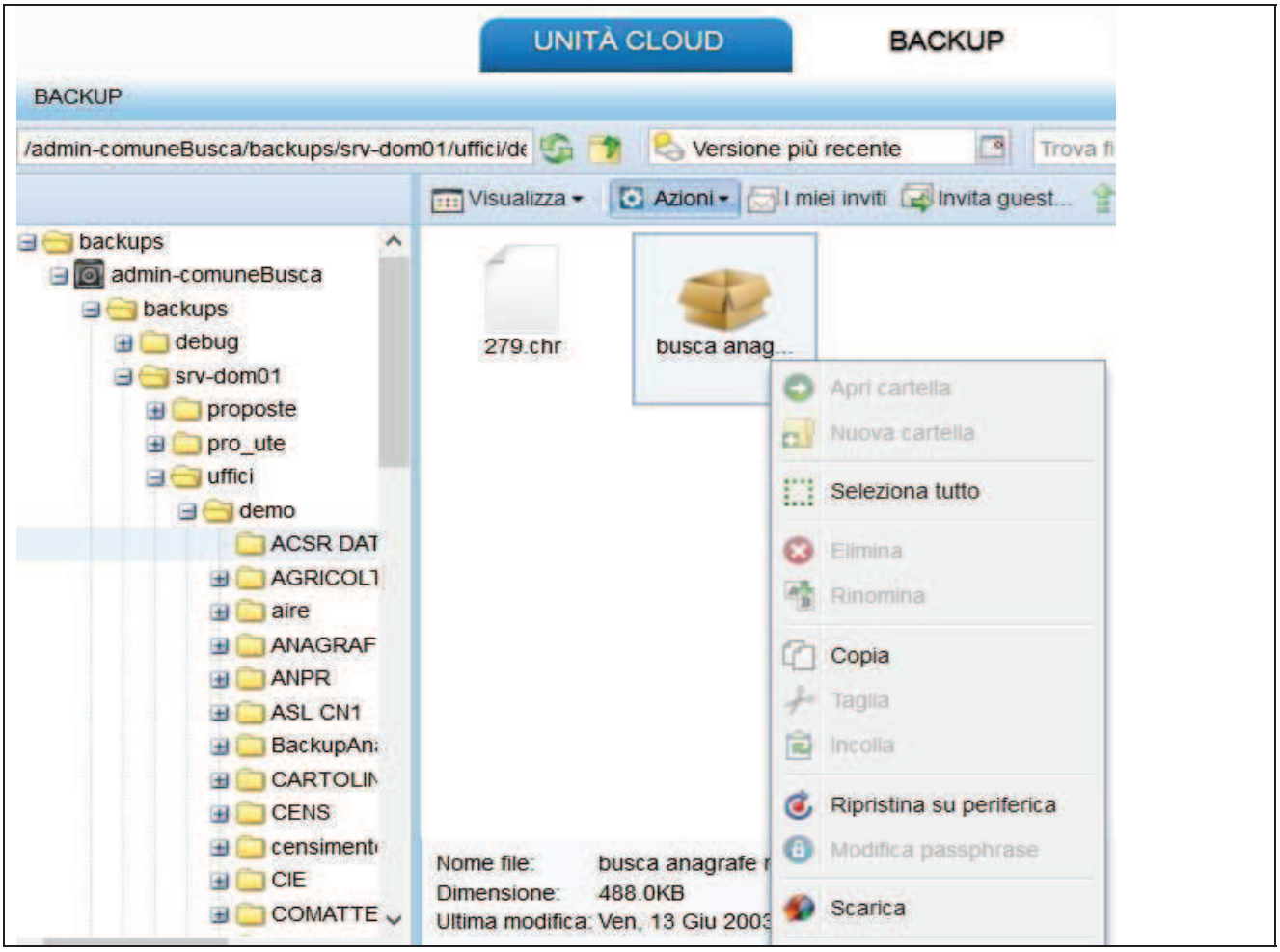
3.16.5 Ripristino tramite cluod

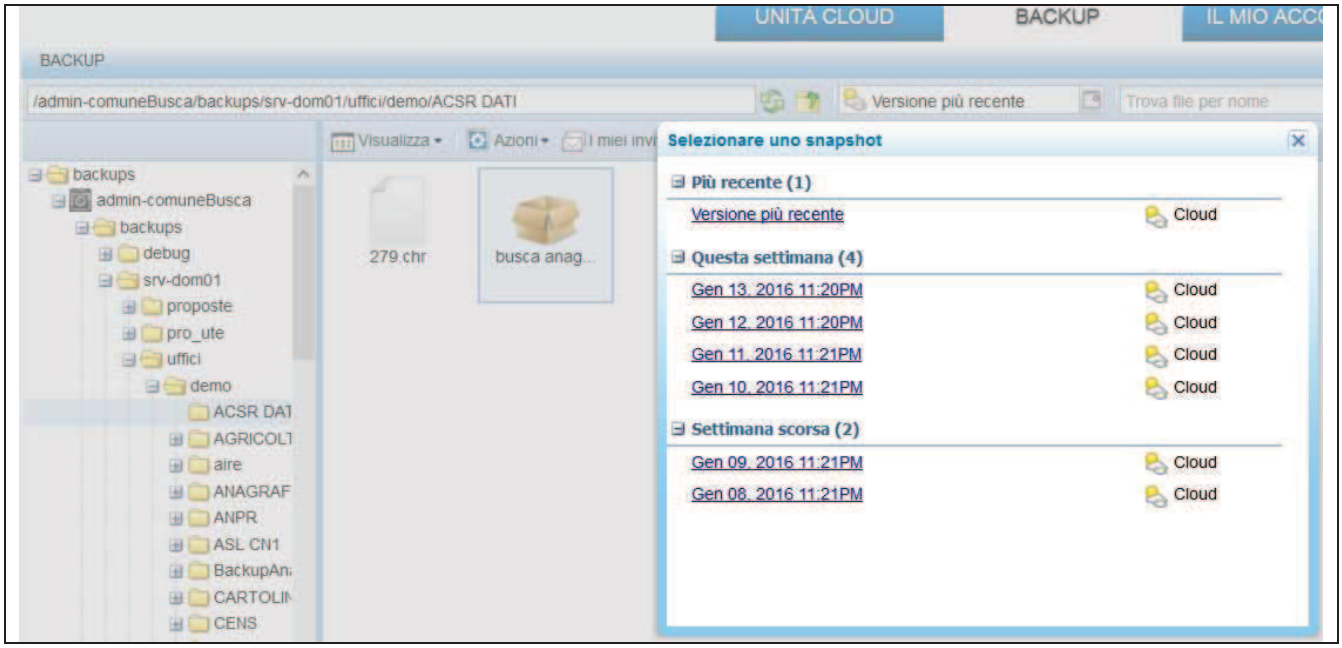
Dopo aver fatto l'accesso remoto, per eseguire il ripristino di un file deve essere selezionata la linguetta backup in alto a destra.

Sul menù di sinistra si seleziona la cartella del file da ripristinare e si sceglie il file nella lista presente a destra.

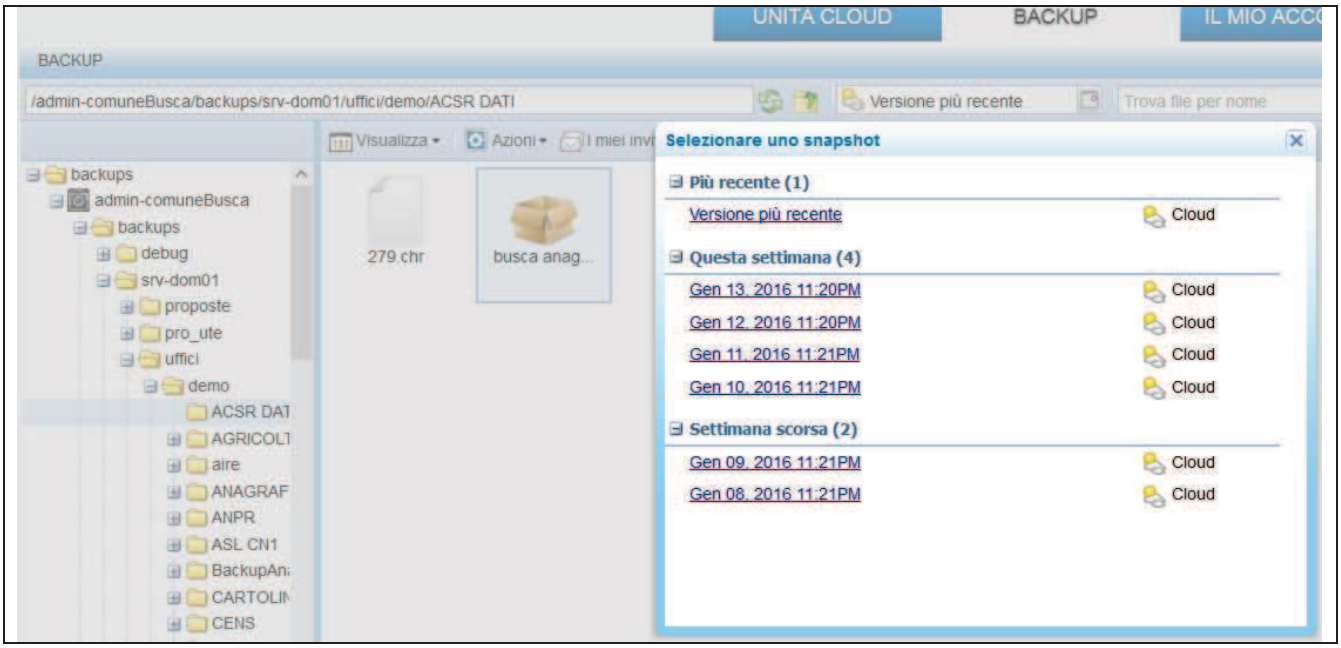
A questo punto dal menù azioni abbiamo disponibili lo “scarica” o la “ripristina su periferica”. Le stesse scelte si possono fare per file singoli o per intere cartelle.

Nelle immagini sottostanti sono presenti le videate con tutte le scelte.



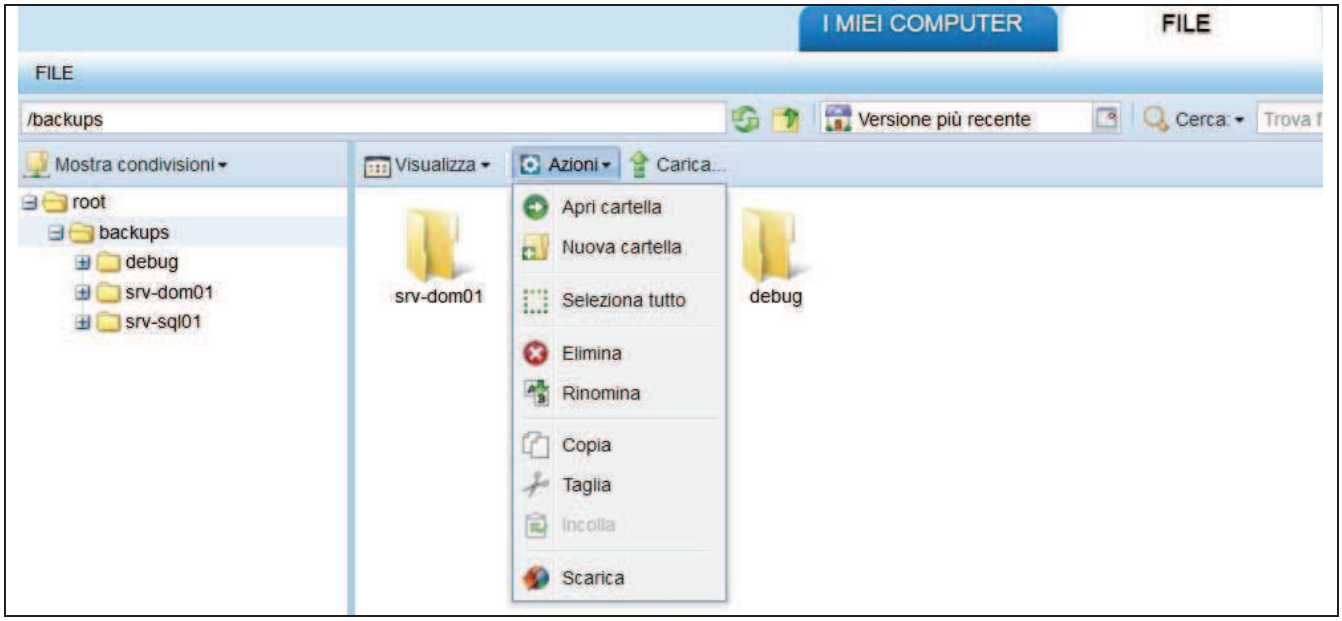


E' possibile scegliere tra le diverse versioni "storicizzate" agendo campo di scelta "versione più recente" e selezionando tra le diverse date presenti. Come da immagine sottostante.



3.16.6 Ripristino locale

Dopo aver fatto l'accesso locale, per eseguire il ripristino di un file deve essere selezionata la linguetta file in alto a destra.
Sul menù di sinistra si seleziona la cartella del file da ripristinare e si sceglie il file nella lista presente a destra.
A questo punto dal menù azioni abbiamo disponibili lo "scarica"
Le stesse scelte si possono fare per file singoli o per intere cartelle. Nelle immagini sottostanti sono presenti le videate con tutte le scelte.



3.6 Fase di ritorno alla normalità

Il rientro dall'emergenza è nelle facoltà del **Comitato di Gestione Crisi** che si riunisce per la valutazione del disastro, per la dichiarazione dell'emergenza, per prendere le decisioni durante tutto l'arco temporale dell'emergenza e al termine della stessa per decidere sul rientro, dopo aver valutato le condizioni di ripristino del sistema informativo comunale e aver ripreso l'erogazione dei servizi.
La dichiarazione di rientro dall'emergenza sarà fatta nel momento in cui l'erogazione dei servizi ai cittadini abbia raggiunto livelli tali da garantire l'accesso a dati e strutture che consentano il normale svolgimento dell'attività lavorativa. Per normale svolgimento dell'attività lavorativa si intende il totale accesso alle strutture, ai dati e al sistema informatico che non pregiudichi l'erogazione dei servizi ovvero si possa ritornare alle attività come venivano svolte precedentemente alla dichiarazione di disastro e/o emergenza.

Il Comitato di Gestione Crisi per poter decretare il ritorno alla normalità dovrà **verificare posivamente** nel

sito Primario:

- La sicurezza statica/agibilità degli edifici
- La continuità di erogazione elettrica
- Il funzionamento degli impianti di riscaldamento/condizionamento (in special modo se previsti per il condizionamento dei locali adibiti al posizionamento degli apparati server/storage)
- Il funzionamento degli apparati hardware di collegamento e dell'hardware installato centralmente e negli uffici (postazioni client)
- Il funzionamento della postazione Server/dei Sever virtuali
- Il funzionamento e il collegamento in rete di tutte le postazioni Client
- Il funzionamento delle policy di sicurezza dell'Ente (antivirus, credenziali di accesso riservate, firewall, ecc)
- Il funzionamento della connessione internet
- Il funzionamento dei software necessari alla gestione dei servizi (sia sul sever che sui singoli client)
- Il funzionamento degli apparati esterni in dotazione ai client necessari ai servizi (scanner, stampanti, plotter, ecc.)
- Il funzionamento del backup ripristinato dalla sede secondaria.

Il Comitato di Gestione Crisi potrà alternativamente decretare il sito alternativo secondario a nuovo sito primario qualora le condizioni di ripristino della sede Primaria non risultino possibili/convenienti.

Il Comitato di Gestione Crisi provvederà ad informare i Responsabili delle Aree coinvolte sul momento di rientro alla sede abituale e/o ad una diversa sede in caso di indisponibilità di quella principale.

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 attivita' sia ordinarie sia di emergenza. E' compito del Responsabile della Continuita' 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 Gestione e aggiornamento del piano di continuita' operativa

5.1 Modalità di esecuzione dei test periodici

La responsabilità dell'esecuzione dei test di continuità operativa è dell'Amministrazione. I tecnici di AeC Servizi della sede di Cuneo potranno fornire assistenza durante queste fasi, secondo quando opportunamente concordato con l'amministrazione.

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

Sono possibili varie tipologie di modalità di test, da eseguirsi anche contemporaneamente, nel corso di un anno che comprendono sia l'aspetto teorico che quello pratico.

La prima tipologia di test la più semplice, ma da attuarsi come prima, è quella di verificare se tutti gli aspetti necessari per attuare la continuità operativa risultano presenti nel documento (es nomina dei responsabili, funzionamento degli impianti del sito secondario, ecc) fattibile predisponendo una check list apposita.

Per quanto riguarda l'aspetto teorico o simulazione o test "walktrought" tale prova verrà realizzata senza l'attivazione fisica dei sistemi ma coinvolgendo tutto il personale che da piano deve essere coinvolto risultando un utile aspetto formativo particolare dell'attività di Continuità Operativa.

Infine la tipologia di test più completo prevede l'effettiva attivazione di impianti e il coinvolgimento delle risorse fisiche e tecnologiche della realtà comunale a fronte di una simulazione di emergenza.

Ricordando che è obbligatorio svolgere almeno un test all'anno in funzione delle esigenze dell'Amministrazione potranno essere eseguiti anche ulteriori test.

5.2 Modalità di revisione e adeguamento del piano

Il piano di Continuità Operativa deve essere aggiornato entro il 31 dicembre di ogni anno come indicato dall'articolo 50 bis del D.Lgs 82/2005.

Di seguito riportiamo le regole operative a cui attenersi per l'aggiornamento delle documentazioni:

- La modifica apportata ad un qualsiasi documento che costituisce il Piano di Continuità ne comporterà un'aggiornamento/release
- La modifica di un manuale o di un allegato derivante da manutenzione ordinaria darà luogo ad un aggiornamento minore o relase la numerazione del documento verrà aggiornata per il suo aspetto di numerazione secondaria (ad esempio passando dall 1.0 alla 1.1)
- La modifica di un manuale o di un allegato derivante da manutenzione straordinaira darà luogo ad un aggiornamento importante che porterà all'aumento del numero primario del manuale (ad esempio passando dalla 1.8 alla 2.0)

La numerazione deve essere modificata sul frontespizio delle documentazioni aggiornando anche la data di stesura della stessa e salvata nel formato informatico definito.

A titolo di esempio si riportano di seguito alcune tipologie di eventi che devono essere presi in considerazione per l'adeguamento del PCO ICT:

- modifiche nella composizione della/e struttura/e organizzava/e (Comitato di gestione della crisi ICT, resp. CO ICT, gruppi di supporto, ecc.) preposte alla gestione della continuità operativa ICT;
- modifiche nei dati personali e/o di reperibilità
- modifiche dei fornitori e/o del contratto assicurativo
- modifiche dei servizi o delle applicazioni software (aggiunta o eliminazione di applicazioni, variazioni nella criticità delle applicazioni)
- modifiche nell'hardware e/o nella rete
- modifiche nella logistica
- stipula di nuovi contratti

E' comunque necessario che almeno una volta all'anno, in concomitanza o meno con il test, il Comitato di crisi si riunisca per analizzare la completezza e attualità del PCO ICT.

La nuova copia della documentazione cartacea dovrà essere firmata per approvazione dal responsabile del Gruppo di supporto unitamente alla data di approvazione dello stesso.

Ad ogni nuova versione della documentazione deve essere curata dal comitato di crisi la distribuzione delle copie del documento a tutti gli interessati inseriti all'interno della modulistica iniziale.