COPIA

CITTÁ DI SORSO

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N. 54 del 08.04.2014

Oggetto: Presa d'atto parere n.798/2013 di AGID (Agenzia per l'Italia Digitale) reso ai sensi dell'art.50 bis del D.lgs.n.82 del 07.03.2005. Definizione dei piani di Continuità Operativa e di Disaster Recovery. Indirizzi agli uffici per la realizzazione delle soluzioni. Modifica organi di gestione della continuità operativa.

L'anno duemilaquattordici, il giorno 08 del mese di Aprile dalle ore 08.00 nella Casa Comunale, si è riunita la Giunta presieduta dal Dr. Giuseppe Morghen, nella sua qualità di Sindaco, e con l'intervento dei Sigg. Assessori:

	P	A
Pulino Giovanna Maria	X	
Pietri Simonetta	X	
Cattari Giuseppe Giovanni Maria	X	
Delogu Agostino	X	
Demelas Fabrizio	X	
Vacca Mauro	X	
Sias Giacomino	X	

Partecipa alla seduta il Segretario Generale Dr. Walter Enzo Marchetiello.

Constatata la legalità dell'adunanza per il numero degli intervenuti, il Presidente dichiara aperta la seduta.

L A G I U N T A

Visto il D.Lgs n.235 del 30/12/2010, recante modificazioni ed integrazioni al D.Lgs n.82 del 07/03/2005 conosciuto come "Codice dell'Amministrazione Digitale", introducendo, con l'articolo 34 comma 2, l'Art. 50-bis, il concetto di Continuità Operativa che vincola le Pubbliche Amministrazioni a definire, nell'ambito della disponibilità dei dati alla base dei servizi, dei piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il ritorno alla normale operatività, il tutto in omogeneità di soluzione garantita dal comma 4 del predetto articolo, che obbliga il DigitPA (ex CNIPA) ad acquisire un parere sui piani predisposti dalla singola amministrazione;

Evidenziato che, a tali fini, le pubbliche amministrazioni definiscono:

- a. il piano di continuità operativa, che fissa gli obiettivi e 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 e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

Dato atto che:

la lett. a) del comma 3 dell'art. 50-bis impone dunque alle Pubbliche Amministrazioni di definire il ***piano di continuità operativa*** (la cui funzionalità deve essere verificata con cadenza almeno biennale) e che deve contenere la descrizione delle relative procedure da seguire, tenendo conto delle risorse umane, strutturali e tecnologiche di ciascuna realtà amministrativa e delle idonee misure preventive;

- la lett.b) del comma 3 del medesimo articolo sancisce l'obbligo per le pubbliche amministrazioni di delineare altresì un **piano di disaster recovery**, che costituisce parte integrante del piano di Continuità Operativa di cui alla lettera precedente e che fissa quali misure tecniche e organizzative, le pubbliche amministrazioni debbano adottare per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione DigitPA, 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
- Attraverso tale introduzione il legislatore prende atto di come l'intenso utilizzo della tecnologia nell'ambito dell'attività istituzionale degli enti, debba essere accompagnato necessariamente dalla predisposizione di piani di emergenza che assicurino la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività a seguito di un evento disastroso;

Richiamata la circolare n.58/2011 del DigitPA ove si emanano direttive e metodi attuativi alla Pubbliche Amministrazioni al fine di redigere lo Studio di Fattibilità Tecnica e modalità di invio per il rilascio del relativo parere;

- In particolare, la prima parte della Circolare riporta le informazioni che le Amministrazioni devono inviare a DigitPA ai fini del rilascio del parere sugli Studi di Fattibilità Tecnica (SFT) e le modalità di presentazione delle richieste come previsto dal comma 4 art. 50 bis del CAD;
- La seconda parte della Circolare riporta le informazioni che le Amministrazioni devono inviare a DigitPA ai fini dell'attività di verifica del costante aggiornamento dei Piani di Disaster Recovery (DR), previste dal comma 3, lettera b) art. 50 bis, del CAD;

Richiamato il documento del DigitPA denominato "Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni" pubblicato in data 26/06/2011, le quali descrivono con dettaglio tutti gli

strumenti per ottemperare agli obblighi derivanti dall'Art. 50-bis del CAD, a partire da un percorso di autovalutazione, dalla metodologia per l'individuazione dei rischi (Business Impact Analist BIA) al fine di produrre uno studio di fattibilità tecnica contenente un Piano di Continuità ed un Piano di Disaster Recovery, da presentare al DigitPA stesso per poi implementare le soluzioni previste nei piani anche sulla base dei pareri espressi dal DigitPA;

Considerato che con decreto legge n. 83, convertito nella legge n. 134/2012, è stata istituita l'Agenzia per l'Italia Digitale (AGID). I compiti dell'Agenzia sono definiti in primo luogo dalle competenze degli enti che essa ha assorbito nel momento della loro soppressione: il Dipartimento Digitalizzazione e Innovazione della Presidenza del Consiglio, l'Agenzia per la diffusione delle tecnologie per l'innovazione, DigitPA, l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione per le competenze sulla sicurezza delle reti, e in secondo luogo dalle prescrizioni contenute nel decreto legge n. 179, convertito nella legge n. 221 del 2012;

Dato atto che l'Agenzia per l'Italia Digitale (AgID) ha pubblicato la nuova versione – aggiornata al 2013 - delle "Linee Guida per il Disaster Recovery (DR) delle PA", la quale introduce:

- aggiornamenti e chiarimenti sul ruolo della continuità operativa e sull'importanza delle soluzioni di DR
- precisazioni sui livelli di soluzioni tecnologiche (Tier) adottati convenzionalmente per ciascuna classe di criticità della pubblica amministrazione e le caratteristiche dei Data Center
- chiarimenti su ruoli e responsabilità necessari alla gestione delle soluzioni di DR, con particolare riferimento al ruolo del responsabile della continuità operativa
- precisazioni sugli aspetti e servizi minimi essenziali di cui tener conto, dal punto di vista dell'evoluzione del contesto tecnologico
- nuovi format di "Studio di fattibilità" e di "Piani di Continuità Operativa e di Disaster Recovery" e suggerimenti sugli accorgimenti da adottare per supportare le amministrazioni nella formulazione delle richieste di parere
- informazioni sulle principali criticità e raccomandazioni emerse nelle attività di supporto agli studi di fattibilità tecnica.

Considerato che le principali attività relative alla Continuità operativa vengono affidate al soggetto Responsabile della Continuità Operativa il quale ha il ruolo di supportare l'Amministrazione per predisporre tutte le misure necessarie per ridurre l'impatto di un'emergenza ICT e reagire prontamente e in maniera efficace in caso di una interruzione delle funzioni ICT, a supporto dei servizi erogati, dovuta a un disastro. Inoltre ha la responsabilità' di sviluppare e mantenere aggiornato il PCO. Il Responsabile della Continuità Operativa è anche membro del Comitato di crisi.

Dato atto che ai sensi del punto 3.5.3 delle "Linee Guida per il Disaster Recovery (DR) delle PA" – aggiornate al 2013 al **Responsabile della Continuità Operativa** compete:

<u>durante la condizione di normalità operativa dell'ICT</u>

- predisporre o coordinare la predisposizione dello Studio di Fattibilità Tecnica e della relazione sullo stato di attuazione del CAD;
- curare l'invio della richiesta di parere secondo le modalità previste dalla circolare n. 58;
- mantenere i rapporti con l'Agenzia Italia Digitale, in particolare per gli adempimenti relativi al SFT ed agli aggiornamenti periodici del PCO e del PDR;
- interagire con i diversi settori dell'Amministrazione per individuare le migliori soluzioni tecniche, procedurali e organizzative da implementare nel PCO;
- sviluppare e mantenere aggiornato il PCO e il PDR;
- pianificare e coordinare i test di Continuità Operativa e produrre la reportistica necessaria;
- collaborare con i servizi ICT per aggiornare le procedure tecniche e verificare il corretto funzionamento dei sistemi di disaster recovery;
- assicurare che i percorsi formativi per il personale coinvolto nelle attività di ripristino e rientro descritte nel PCO siano opportunamente seguiti;

- avviare un processo di valutazione di impatto sul PCO, per i cambiamenti tecnici e organizzativi che coinvolgono l'Amministrazione.

Durante lo stato di emergenza ICT

- costituire il punto di riferimento/contatto per la segnalazione dello stato di emergenza ICT (reale o potenziale);
- effettuare valutazioni qualitative e quantitative dell'impatto reale o potenziale che lo stato di emergenza ICT segnalato provoca/può provocare, individuando il personale, i servizi e gli utenti coinvolti per proporre al Comitato di Crisi la dichiarazione dello stato di emergenza;
- richiedere la convocazione del Comitato di Crisi per la valutazione della dichiarazione dello stato di emergenza ICT, fornendo tutte le informazioni necessarie alle decisioni;
- in caso di dichiarazione di emergenza ICT da parte del Comitato di Crisi coordinare i team operativi per la gestione dell'emergenza e per il processo di ritorno alla normalità;
- aggiornare costantemente il Comitato di Crisi ICT durante le varie fasi di gestione dell'emergenza ICT;
- informare il Comitato di Crisi della conclusione delle condizioni dell'emergenza ICT;
- in caso di dichiarazione di conclusione dell'emergenza ICT da parte del Comitato di Crisi curare tutte le operazioni di ritorno alla normalità.

Considerato che in occasione dell'apertura dello stato di emergenza ICT sono affidate all'organismo di vertice denominato Comitato di Crisi le principali decisioni e la supervisione delle attività delle risorse coinvolte; Esso è l'organo di direzione strategica dell'intera struttura e, inoltre, condivide con il responsabile della CO la responsabilità di garanzia e controllo sulla continuità operativa di un Ente o Amministrazione

Dato atto che ai sensi del punto 3.5.4 delle "Linee Guida per il Disaster Recovery (DR) delle PA" – aggiornate al 2013 al **Comitato di Crisi** compete:

I principali compiti del Comitato di Crisi in condizioni ordinarie sono:

- definizione ed approvazione del PCO;
- approvazione degli aggiornamenti al PCO;
- promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità operativa del personale dell'amministrazione.

I principali compiti del Comitato di Crisi, in condizioni di emergenza ICT sono:

- valutazione delle situazioni di emergenza ICT e dichiarazione dello stato di emergenza ICT;
- avvio delle attività di ripristino delle funzionalità informatiche e controllo del loro svolgimento;
- rapporti con l'esterno e comunicazioni ai dipendenti;
- attivazione e monitoraggio del processo di rientro dall'emergenza ICT;
- gestione di tutte le situazioni non contemplate;
- gestione dei rapporti interni e risoluzione dei conflitti di competenza;
- dichiarazione di conclusione dello stato di emergenza ICT.

Dato atto che con delibera di G.C. n. 28 del 22.03.2011 l'Amministrazione Comunale ha redatto per l'anno 2011 il "Documento Programmatico sulla Sicurezza per l'adozione delle misure di sicurezza nel trattamento dei dati personali, ai sensi dell'art.34 del D.Lgs. 196/03";

Ricordato che con provvedimento del 27 novembre 2008, pubblicato in G.U. n. 300 del 24/12/2008, il Garante per la protezione dei dati personali ha imposto ai titolari di trattamento di dati personali e quindi anche ai Comuni, di predisporre un elenco degli amministratori di sistema;

Considerato che nel DPS approvato con delibera di G.C. n. 28 del 22.03.2011 il sig. Antonio Cappai assegnato all'Ufficio Ced risultava incaricato della funzione di "Amministratore di Sistema" ai sensi

del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, pubblicato in G.U. n. 300 del 24/12/2008;

Preso atto che con il decreto-Legge "Disposizioni urgenti in materia di semplificazione e sviluppo" del 03/02/2012, n.5 (pubblicato in Gazzetta Ufficiale n. 33 del 09/02/2012), sono stati modificati l'art.34 e l'Allegato B del D.Lgs. 196/03, in materia di protezione dei dati personali: in particolare risulta eliminato l'obbligo di predisporre e aggiornare il documento programmatico sulla sicurezza (DPS) entro il 31/03/2012, nonchè riferire nella relazione accompagnatoria di bilancio in merito alla sua stesura;

Visto il decreto del Sindaco n.9 del 25.09.2012 prot.14930 con il quale si è provveduto a nominare il sig. Antonio Cappai nato a Sassari il 30.12.1967 residente a Sorso in via Sassari n.14, in qualità di Amministratore di Sistema del Comune di Sorso, ai sensi e per gli effetti del D.lgs.196/2003 e del Provvedimento del Garante Privacy del 27 novembre 2008;

Considerato che, l'espletamento delle funzioni di amministratore di sistema, secondo quanto previsto dall'allegato B del Codice in Materia di Protezione dei Dati Personali D.Lgs. 196/2003, comporta l'adozione di tutte le misure necessarie a tutelare la salvaguardia dei dati Personali, nonché l'adozione di tutti gli adempimenti finalizzati alla sicurezza delle banche dati e alla corretta gestione delle reti telematiche, con funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti istituzionali, e compiti di vigilanza sul corretto utilizzo dei sistemi informatici

Richiamata la Delibera di Giunta Comunale n 162 del 06.11.2012 con la quale si era proceduto:
- alla nomina del Responsabile della Continuità operativa
- alla costituzione del Comitato di gestione della crisi
- all'affidamento a FATICONI SPA della redazione dello Studio di Fattibilità Tecnica per la Continuità Operativa (CO) il Disaster Recovery (DR)

Ritenuto opportuno e necessario, in occasione della definizione dei Piani per la Continuità Operativa (CO) e per il Disaster Recovery (DR), procedere a rimodulare gli organi e le strutture di vertice dell'Amministrazione preposte alla gestione dell'emergenza ICT (Information and Communication Technology), in coerenza con il vigente assetto organizzativo dell'Ente e in adesione alle indicazioni - delle "Linee Guida per il Disaster Recovery (DR) delle PA" aggiornate al 2013, e al D.Lgs. 30.12.2010, n. 235, secondo la seguente organizzazione:

Responsabile della Continuità Operativa	Dirigente 3° settore Dott. Pietro Nurra per il tramite di ufficio di supporto costituito da: - Responsabile in PO AA.GG. - Amministratore di sistema
Responsabile Disaster Recovery	Amministratore di sistema: sig. Antonio Cappai
Comitato di Gestione della Crisi da linee guida: - 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 (se presente); - il responsabile dell'informatica dell'ente (se previsto dall'organizzazione dell'ente); - il responsabile della sicurezza dell'ente, come previsto dalla 81/2008.	- Sindaco del Comune di Sorso - Segretario Generale - Dirigente in carica del 1° Settore – area finanziaria - Dirigente in carica del 2° settore – area tecnica - Dirigente in carica del 3° settore – area amministrativa - Responsabili in PO - Responsabile della continuità operativa - Amministratore di sistema - Responsabile della Protezione Civile - Responsabile della sicurezza

	dell'ente, come previsto dal D.Lgs 81/2008.

Richiamata la Delibera di Giunta Comunale n 136 del 16.07.2013 con la quale si era proceduto:

- all'approvazione dello Studio di Fattibilità Tecnica per la Continuità Operativa (CO) e il Disaster Recovery (DR) e delle Schede di autovalutazione;
- ad incaricare il Responsabile della Continuità Operativa, per il tramite dell'ufficio CED, di trasmettere all'Agenzia per l'Italia Digitale (AGID) (già DIGIT PA,) lo Studio di Fattibilità e i documenti allegati," per la richiesta di parere come previsto dal comma 4 art. 50 bis del CAD

Dato atto che in data 24.07.2013 era stata regolarmente inviata la documentazione all'Agenzia per l'Italia Digitale (AGID) ai fini del rilascio del parere, e preso atto che AGID aveva espresso il parere favorevole n.798/2013 sullo Studio di Fattibilità Tecnica per la Continuità Operativa (CO) e il Disaster Recovery (DR) a condizione che:

1. l'Amministrazione verifichi presso la propria Regione, prima di dare avvio alla Soluzione, la presenza di piani regionali conseguenti a quanto disposto dall'art.33 – septies del D.L. 179 convertito nella legge 221/2010;
2. 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
3. La soluzione tecnica di continuità operativa garantisca l'Amministrazione da tutti gli scenari di crisi potenziali
4. 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 si ripristino (RTO) e di perdita massima di dati accettata (RPO)

Dato atto che le soluzioni di continuità operativa e Disaster Recovery individuate dalle "Linee Guida per il Disaster Recovery (DR) delle PA" – aggiornate al 2013 sono convenzionalmente indicate con il termine "Tier" - (letteralmente, livello, grado) che classifica n.6 livelli di soluzioni progressivamente migliorative, in relazione alla classe di criticità operativa dei servizi;

Considerato che la soluzione tecnica indicata dall'Amministrazione Comunale per i servizi in ambito corrisponde a "**Tier 4"** : la soluzione prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. Le altre caratteristiche sono quelle del Tier 3, con la possibilità di aggiornamento dei dati (RPO) con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono).

Considerato che, ai sensi del punto 2.4 e 6 delle "Linee Guida per il Disaster Recovery (DR) delle PA" – aggiornate al 2013, le Amministrazioni, una volta acquisito il parere obbligatorio dell'Agenzia per l'Italia Digitale sullo studio di fattibilità tecnica, devono:

- definire conseguentemente i Piani per descrivere le misure organizzative e tecniche di cui intendono dotarsi per garantire la CO e il DR";
- procedere all'acquisizione delle infrastrutture tecnologiche e delle risorse software necessarie a rendere operativi il PCO e il PDR adottati.

Dato atto che l'Ufficio Ced ha verificato l'assenza, presso la Regione Sardegna, di piani regionali conseguenti a quanto disposto dall'art.33 – septies del D.L. 179/2012 convertito nella legge 221/2012 il quale testualmente recita:

Art. 33-septies. Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese

- 1. L'Agenzia per l'Italia digitale, con l'obiettivo di razionalizzare le risorse e favorire il consolidamento delle infrastrutture digitali delle pubbliche amministrazioni, avvalendosi dei principali soggetti pubblici titolari di banche dati, effettua il censimento dei Centri per l'elaborazione delle informazioni (CED) della pubblica amministrazione, come definiti al comma 2, ed elabora le linee guida, basate sulle principali metriche di efficienza internazionalmente riconosciute, finalizzate alla definizione di un piano triennale di razionalizzazione dei CED delle amministrazioni pubbliche che dovrà portare alla diffusione di standard comuni di interoperabilità, a crescenti livelli di efficienza, di sicurezza e di rapidità nell'erogazione dei servizi ai cittadini e alle imprese.
- 2. Con il termine CED è da intendere il sito che ospita un impianto informatico atto alla erogazione di servizi interni alle amministrazioni pubbliche e servizi erogati esternamente dalle amministrazioni pubbliche che al minimo comprende apparati di calcolo, apparati di rete per la connessione e apparati di memorizzazione di massa.
- 3. Dalle attività previste al comma 1 sono esclusi i CED soggetti alla gestione di dati classificati secondo la normativa in materia di tutela amministrativa delle informazioni coperte da segreto di Stato e di quelle classificate nazionali secondo le direttive dell'Autorità nazionale per la sicurezza (ANS) che esercita le sue funzioni tramite l'Ufficio centrale per la segretezza (UCSe) del Dipartimento delle informazioni per la sicurezza (DIS).
- 4. Entro il 30 settembre 2013 l'Agenzia per l'Italia digitale trasmette al Presidente del Consiglio dei ministri, dopo adeguata consultazione pubblica, i risultati del censimento effettuato e le linee guida per la razionalizzazione dell'infrastruttura digitale della pubblica amministrazione. Entro i successivi novanta giorni il Governo, con decreto del Presidente del Consiglio dei ministri, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta il piano triennale di razionalizzazione dei CED delle pubbliche amministrazioni di cui al comma 1, aggiornato annualmente.
- 4-bis. Nell'ambito del piano triennale di cui al comma 4 sono individuati i livelli minimi dei requisiti di sicurezza, di capacità elaborativa e di risparmio energetico dei CED, nonché le modalità di consolidamento e razionalizzazione, ricorrendo ove necessario all'utilizzo dei CED di imprese pubbliche e private nonché di enti locali o di soggetti partecipati da enti locali nel rispetto della legislazione vigente in materia di contratti pubblici.
- (comma introdotto dall'art. 16 della legge n. 98 del 2013)
- 5. Dall'attuazione del presente articolo non derivano nuovi o maggiori oneri o minori entrate per il bilancio dello Stato.

Visto l’allegato Piano per la Continuità Operativa (CO) e il Disaster Recovery (DR) predisposto dall’Ufficio Ced sulla base dello Studio di Fattibilità Tecnica (SFT) approntato dalla società Faticoni Spa e del parere favorevole n.798/2013 all'Agenzia per l'Italia Digitale (AGID) e dato atto che lo stesso può essere approvato da parte del “Comitato di Gestione di Crisi”;

Ritenuto pertanto di procedere a:

- prendere atto dell’allegato Piano per la Continuità Operativa (CO) e il Disaster Recovery (DR) predisposto sulla base dello Studio di Fattibilità Tecnica (SFT) e del parere favorevole n.798/2013 all'Agenzia per l'Italia Digitale (AGID);
- demandare al Comitato di gestione della Crisi l’approvazione dell’allegato Piano per la Continuità Operativa (CO) e il Disaster Recovery (DR)
- inviare il predetto Piano, in formato elettronico, mediante posta elettronica certificata (PEC) (indirizzo PEC:Digitpadir@pec.digitpa.gov.it) per il tramite del Responsabile della Continuità Operativa, dalla casella PEC dell’Amministrazione (circolare n.58/2011 del DigitPA parte seconda)
- Incaricare il Responsabile della Continuità Operativa dell’invio a DigitPA con cadenza annuale, entro il 31 dicembre di ogni anno, mediante posta elettronica certificata (PEC) a (indirizzo PEC: Digitpadir@pec.digitpa.gov.it), dalla casella PEC della Amministrazione, della versione aggiornata del Piano di DR in formato elettronico unitamente alla dichiarazione che,

in relazione al Piano di DR trasmesso in precedenza, specifichi le modifiche intervenute e le motivazioni di tali modifiche, utilizzando lo schema indicato nella circolare n.58/2011 del DigitPA parte seconda:

- impartire indirizzi agli uffici ed assegnare le risorse economiche quantificate in € 70.000,00, da ripartire nelle annualità 2014 e 2015, per l'avvio delle soluzioni tecniche individuate nel suddetto Piano per la Continuità Operativa (CO) e Disaster Recovery (DR) da realizzare mediante l'acquisizione delle infrastrutture tecnologiche e delle risorse software necessarie a rendere operativi il PCO e il PDR adottati
- impartire indirizzi agli uffici ed assegnare le risorse economiche quantificate in € 9.000,00 al fine di procedere in ordine ai lavori di sistemazione dei locali individuati ad ospitare i server di replica e backup dell'infrastruttura informatica Comunale, mediante la realizzazione delle tramezzature, porte blindate, condizionatori, impianto elettrico, in aderenza alle soluzioni individuate nel Piano per la Continuità Operativa (CO) e Disaster Recovery (DR);

Dato atto che agli interventi suddetti si farà fronte con imputazione ai seguenti capitoli di bilancio:

- **Avvio soluzioni tecniche. Acquisizione infrastrutture tecnologiche e risorse software**
  capitolo n.10778 denominato "Spesa per potenziamento/ampliamento rete informatica comunale"
  Esercizio 2014 € 45.000,00
  Esercizio 2015 € 25.000,00
- **lavori di sistemazione locali individuati ad ospitare i server di replica e backup**
  capitolo n.18411 denominato "Macchine, software di automazione d'ufficio, attrezzature e arredi ufficio urbanistica."
  Esercizio 2014 € 9.000,00

Ritenuto opportuno procedere in merito;

Ritenuta la proposta meritevole di accoglimento;

Visto il parere favorevole di regolarità tecnica e contabile espresso ai sensi dell'art.49, comma 1, del D.Lgs. n.267/2000 e incluso in calce alla presente deliberazione, dal Dirigente Responsabile del Servizio Finanziario, e Affari Generali Dott. Pietro Nurra;

A VOTI unanimi, espressi a scrutinio palese,

D E L I B E R A

1) Di prendere atto e di approvare quanto in premessa;
2) Di prendere atto del parere favorevole n.798/2013 espresso dall'Agenzia per l'Italia Digitale (AGID) sullo Studio di Fattibilità Tecnica per la Continuità Operativa (CO) e il Disaster Recovery (DR) come previsto dal comma 4 art. 50 bis del CAD;
3) di rimodulare gli organi e le strutture di vertice dell'Amministrazione preposte alla gestione dell'emergenza ICT (Information and Communication Technology), in coerenza con il vigente assetto organizzativo dell'Ente e in adesione alle indicazioni - delle "Linee Guida per il Disaster Recovery (DR) delle PA" aggiornate al 2013, e al D.Lgs. 30.12.2010, n. 235, secondo la seguente organizzazione:

Responsabile della Continuità Operativa	Dirigente 3° settore Dott. Pietro Nurra per il tramite di ufficio di supporto costituito da: - Responsabile in PO AA.GG. - Amministratore di sistema
Responsabile Disaster Recovery	Amministratore di sistema: sig. Antonio Cappai

Comitato di gestione della crisi da linee guida: - 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 (se presente); - il responsabile dell'informatica dell'ente (se previsto dall'organizzazione dell'ente); - il responsabile della sicurezza dell'ente, come previsto dalla 81/2008.	- Sindaco del Comune di Sorso - Segretario Generale - Dirigente in carica del 1° Settore – area finanziaria - Dirigente in carica del 2° settore – area tecnica - Dirigente in carica del 3° settore – area amministrativa - Responsabili in PO - Responsabile della continuità operativa - Amministratore di sistema - Responsabile della Protezione Civile - Responsabile della sicurezza dell'ente, come previsto dal D.Lgs 81/2008.

4) Di prendere atto dell'allegato Piano per la Continuità Operativa (CO) e il Disaster Recovery (DR) predisposto sulla base dello Studio di Fattibilità Tecnica (SFT) e del parere favorevole n.798/2013 all'Agenzia per l'Italia Digitale (AGID);

5) Di demandare al Comitato di gestione della Crisi l'approvazione dell'allegato Piano per la Continuità Operativa (CO) e il Disaster Recovery (DR)

6) di inviare il predetto Piano, in formato elettronico, mediante posta elettronica certificata (PEC) (indirizzo PEC:Digitpadir@pec.digitpa.gov.it) per il tramite del Responsabile della Continuità Operativa supportato dall'ufficio all'uopo individuato, dalla casella PEC dell'Amministrazione (circolare n.58/2011 del DigitPA parte seconda)

7) di incaricare il Responsabile della Continuità Operativa, supportato dall'ufficio all'uopo individuato, dell'invio a DigitPA con cadenza annuale, entro il 31 dicembre di ogni anno, mediante posta elettronica certificata (PEC) a (indirizzo PEC: Digitpadir@pec.digitpa.gov.it), dalla casella PEC della Amministrazione, della versione aggiornata del Piano di DR in formato elettronico unitamente alla dichiarazione che, in relazione al Piano di DR trasmesso in precedenza, specifichi le modifiche intervenute e le motivazioni di tali modifiche, utilizzando lo schema indicato nella circolare n.58/2011 del DigitPA parte seconda:

8) di incaricare il Responsabile della Continuità Operativa di convocare il Comitato di Crisi con cadenza biennale, per la verifica della funzionalità del Piano per la Continuità Operativa (CO) e l'approvazione degli aggiornamenti, ai sensi della lett. a) comma 3 dell'art. 50-bis. del D.Lgs n.82 del 07/03/2005;

9) Di incaricare il Responsabile del Servizio Affari Generali di procedere all'avvio delle soluzioni tecniche individuate nel suddetto Piano per la Continuità Operativa (CO) e Disaster Recovery (DR), mediante:

a) l'individuazione del fornitore con la miglior proposta tecnico economica di tipo modulare, per l'acquisizione delle infrastrutture tecnologiche e delle risorse software necessarie a rendere operativi il PCO e il PDR medesimi;

b) l'approvazione di progetti che assicurino per tutta la durata del contratto, un servizio di assistenza agli uffici comunali da parte del fornitore medesimo, nonché la manutenzione e l'aggiornamento delle soluzioni adottate. Durante il periodo di emergenza, il fornitore dovrà altresì assicurare l'assistenza operativa ed il presidio a supporto del personale dell'Amministrazione, che è comunque responsabile della conduzione in esercizio dei sistemi;

c) la verifica dell'inserimento nel contratto di servizio con il fornitore delle clausole contrattuali per regolamentare i servizi e le soluzioni di CO/DR nel rispetto delle indicazioni "Linee Guida per il Disaster Recovery (DR) delle PA" adottate dall'Agenzia per l'Italia Digitale (AgID)– nella versione aggiornata al 2013 (D.2" pag 121 ss.);

10) Di assegnare per le finalità di cui al punto 9) l'importo complessivo di € 70.000,00 con imputazione al capitolo n.10778 denominato "Spesa per potenziamento/ampliamento rete informatica comunale" secondo la seguente ripartizione:

Esercizio 2014 € 45.000,00

Esercizio 2015 € 25.000,00

11) Di incaricare il Dirigente del 2° Settore LL.PP. di procedere in ordine ai lavori di sistemazione dei locali individuati ad ospitare i server di replica e backup dell'infrastruttura informatica Comunale, mediante la realizzazione delle tramezzature, porte blindate, condizionatori, impianto elettrico, in aderenza alle soluzioni individuate nel Piano per la Continuità Operativa (CO) e Disaster Recovery (DR);

12) Di assegnare per le finalità di cui al punto 11) l'importo complessivo di € 9.000,00 con imputazione al capitolo n.18411 denominato "Macchine, software di automazione d'ufficio, attrezzature e arredi ufficio urbanistica." esercizio 2014;

13) Di incaricare l'Ufficio Segreteria di trasmettere il presente provvedimento al responsabile della continuità operativa e ai suddetti componenti del Comitato di gestione della crisi;

14) Di dichiarare, con separata e parimenti unanime votazione, la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del d.lgs.vo 267/2000, riconosciuta l'urgenza di assicurare la sollecita attuazione delle sue descritte finalità.

Letto e approvato, il presente verbale viene come in appresso sottoscritto

Dr. Giuseppe Morghen	**Dr. Walter Enzo MARCHETIELLO**
F.TO MORGHEN	**F.TO MARCHETIELLO**
(Il Presidente)	(Il Segretario Generale)

Attestazione parere art.49 D.Lgs 18/08/2000

Regolarità Tecnica:	***Regolarità Contabile***
Parere favorevole	*Parere favorevole*
FIRMATO IL DIRIGENTE **Dr. Pietro Nurra**	FIRMATO IL DIRIGENTE **Dr. Pietro Nurra**

ATTESTAZIONE DI PUBBLICAZIONE NELL'ALBO PRETORIO ON LINE, DI CONTESTUALE COMUNICAZIONE AI SIGG. CAPIGRUPPO, DI INSERIMENTO NEL SITO INTERNET COMUNALE.

Certifico che la presente deliberazione viene pubblicata in data **18 aprile 2014** all'Albo Pretorio On Line al **n. 215** del Registro (art. 124, T.U.E.L.) e contestualmente comunicata ai Capigruppo consiliari (art. 125, T.U.E.L.). La presente deliberazione è altresì pubblicata nel sito istituzionale del Comune di Sorso all'indirizzo: www.comune.sorso.ss.it sezione: Deliberazioni Giunta.
Sorso, **18 Aprile 2014**

Dr. Pietro NURRA

F.TO NURRA
(Il Vice Segretario Generale)

CERTIFICATO DI PUBBLICAZIONE E DI ESECUTIVITÀ

Certifico che la presente deliberazione stata pubblicata mediante inserzione all'Albo Pretorio On Line istituito presso il sito istituzionale del Comune di Sorso all'indirizzo: www.comune.sorso.ss.it per quindici giorni consecutivi dal **18 Aprile 2014**.

Dr. Pietro NURRA

Sorso, li **18 Aprile 2014**

F.TO NURRA
(Il Vice Segretario Generale)

La presente deliberazione, è divenuta esecutiva in data **08.04.2014** poiché dichiarata immediatamente eseguibile, (art. 134, comma 4, T.U.E.L.).

Dr. Pietro NURRA

Sorso, li **18 Aprile 2014**

(Il Vice Segretario Generale)

COPIA CONFORME ALL'ORIGINALE: Sorso, 18 Aprile 2014

Il Vice Segretario Generale
(Dr. Pietro Nurra)