

DELIBERAZIONE DELLA GIUNTA COMUNALE

Copia

N° 84 del Reg.

Data: 26/10/2012

OGGETTO: Adempimenti urgenti per il Disaster Recovery e la Continuità Operativa, alla luce del Decreto Legge 04 ottobre 2012. Sviluppo e Agenda Digitale. Provvedimenti. -

L'anno Duemiladodici (2012), il giorno Ventisei (26), del mese di Ottobre, alle ore 10,00, nella sala delle adunanze del Comune, sotto la presidenza del geom. Franco Martino, nella sua qualità di Sindaco, si è riunita la Giunta Comunale;

Per riunione ordinaria (art. 4 regolamento per il funzionamento della giunta comunale). -

Componenti	Presenti	Assenti	
Geom. Martino Franco	X		Assegnati n.: 5
Sig. Mastrantuono Luigi	X		In Carica n.: 5
Sig. Volpe Emilio		X	Presenti n.: 3
Sig. Scottillo Antonio		X	Assenti n.: 2
Sig. Andresano Tullio	X		Assenti i Signori: -
			Sig. Volpe Emilio - Sig. Antonio Scottillo -

Risultato che gli intervenuti sono in numero legale;

Partecipa con funzioni consultive, referenti, di assistenza e verbalizzazione (art. 97 - comma 4.a, del T. U. E. L. n° 267 / 2000), il Segretario Comunale dr. Fernando Antico;

Il Presidente dichiara aperta la riunione sull'argomento ed invita i convocati a deliberare sull'oggetto sopraindicato, premettendo che, sulla proposta della presente deliberazione i responsabili delle aree interessate hanno espresso il proprio parere, come di seguito riportato:

AREA INTERESSATA	AREA FINANZIARIA
VISTO: si esprime parere FAVOREVOLE in ordine alla regolarità tecnica della presente proposta di deliberazione, ai sensi e per gli effetti dell'art. 49, comma 1°, del T. U. E. L. n° 267/2000. - Dalla Residenza Comunale, 26/10/2012 IL RESPONSABILE DELL'AREA F.to Sig. Ascanio Marino [Amministrativa]	VISTO: ai sensi e per gli effetti dell'art. 49, comma 1° e dell'art. 151, comma 4°, del T. U. E. L. n° 267 / 2000, SI ATTESTA la regolarità contabile della spesa prevista nella presente proposta di deliberazione. Dalla Residenza Comunale, 26/10/2012 IL RESPONSABILE DELL'AREA F.to Dr. Raffaele Poto [Finanziaria]

La Giunta Comunale

Premesso che il Codice dell'Amministrazione Digitale (Decreto legislativo 07 marzo 2005, n° 82, aggiornato alla luce del alla luce del Decreto Legge 22 giugno 2012, n° 83 e 06 luglio 2012, n° 95, convertiti con modificazioni, rispettivamente, dalla Legge 07 agosto 2012, n° 134 e Legge 07 agosto 2012, n° 135 e del Decreto Legge 04 ottobre 2012, sull'Agenda digitale), all'art. 50-bis rubricato "**Continuità operativa**" impone alle Pubbliche Amministrazioni, centrali e locali, di predisporre i piani di **Disaster Recovery** e di **Business Continuity**, a salvaguardia dei servizi erogati a cittadini e imprese.

Dato atto che l'Autorità nazionale per la digitalizzazione delle pubbliche amministrazioni, sentito il Garante per la protezione dei dati personali, ha pubblicato le "Linee guida per il **Disaster Recovery** delle pubbliche amministrazioni, ai sensi del comma 3, lettera b) dell'art. 50-bis - del Decreto Legislativo n° 82/2005 e s.m.i.", nelle quali sono dettagliati 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 Analyst BIA) al fine di produrre uno Studio di Fattibilità Tecnica per il Piano di **Continuità Operativa** e il Piano di **Disaster Recovery**, da presentare all'Autorità stessa, al fine di implementare le soluzioni previste nei piani, anche sulla base dei pareri espressi dalla stessa Autorità Nazionale.

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

Che la Circolare 01 dicembre 2011, n° 58 (G. U. 27/12/2011, n° 300) fornisce le indicazioni necessarie ad adempiere a quanto previsto dal citato articolo 50-bis del CAD e, in particolare, riporta le informazioni che le amministrazioni devono inviare a **DigitPA**, ai fini del rilascio del Parere sugli Studi di Fattibilità Tecnica (SFT), come previsto dal comma 4, nonché le informazioni che le amministrazioni devono inviare ai fini dell'attività di verifica dei Piani di **Continuità Operativa** (CO) e di **Disaster Recovery** (DR), previste dal comma 3, lettere a, b) **obbligatori entro il 31/12/2012**.

Evidenziato che la finalità delle norme è quello di fare in modo che gli enti locali, essendo titolari della generalità delle funzioni amministrative nei confronti dei cittadini e delle imprese e, in quanto **front-end** naturale dell'**e-government**, valutino l'effettiva criticità che comporta l'interruzione dei servizi che erogano a cittadini e imprese e **pianifichino** le soluzioni al fine di garantirne la continuità e il ripristino in tempi ragionevoli in caso di eventi disastrosi.

Ritenuta la necessità di **trasmettere urgentemente** la richiesta di parere obbligatorio all'Agenzia per l'Italia Digitale, istituita dalla Legge 07 agosto 2012, n° 134, sullo **SFT**, corredata da apposita Relazione previsionale e dagli esiti della autovalutazione eseguita mediante lo strumento di cui alle Linee Guida, in ottemperanza all'art. 50 bis del CAD.

Evidenziata altresì la necessità di predisporre, sulla base dello SFT il Piano di **Continuità Operativa** e **Disaster Recovery** ai sensi dell' art. 50 bis del CAD (comma 3, punti a,b) e le idonee misure tecniche e organizzative per l'istruttoria dell'Agenzia per l'Italia Digitale entro la scadenza del **31/12/2012**.

Vista la proposta espressa all'uopo nella nota di **Asmez**, corredata dalla documentazione tecnica inerente ai servizi **IT** infrastrutturali, **consulenziali** e di assistenza "**AsmeCloud**", con particolare riferimento ai servizi **Asmecloud START + BRD + MAN**, che comprendono la progettazione e messa a disposizione della Piattaforma **ICT** per il **Disaster Recovery**, il supporto alla redazione dello Studio di Fattibilità Tecnica (SFT) e al Piano di **Continuità Operativa** e di **Disaster Recovery** (PCO e PDR), e il supporto all'attività istruttoria dell'Agenzia per l'Italia Digitale, per il parere ai sensi dell'art. 50 bis del CAD.

Vista la nota prot. n° 4218 - del 25/10/2012 (allegata alla presente), con la quale il dr. Nicola Pagano, responsabile del servizio **CED** di questo Comune, con la quale propone a questo Organo Esecutivo la redazione dello studio di fattibilità, e quant'altro in essa contenuto.

COMUNE DI AQUARA

PROVINCIA DI SALERNO
Via Garibaldi, 5 - 84020 Aquara (SA)
Tel.: 0828.962003 - Fax: 0828.962110
P.E. Ordinaria: info@comune.aquara.sa.it
P.E.C.: protocollo.amministrazione@pec.comune.aquara.sa.it
Sito Web istituzionale: www.comune.aquara.sa.it
Codice Fiscale: 82001370657

Ufficio CED

COMUNE DI AQUARA (SA)
PRO: Prot. 0004218 del 25-10-2012
in Partenza Ore 13:45:18
DAT: Mitt: Sindaco - SEDE + Segretario C/le-SEDE

A
Al Sig. Sindaco
e, p.c.: al Segretario Generale

Oggetto: Adempimenti urgenti per il Disaster Recovery e la Continuità Operativa dei Comuni alla luce del Decreto-legge 4 ottobre 2012 "Sviluppo e Agenda Digitale".

L'art. 50-bis del Codice dell'Amministrazione Digitale (CAD) rende obbligatoria la pianificazione in materia di continuità operativa e di Disaster Recovery, prevedendo che "in relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività."

Ciascun Comune adottare e gestire nel tempo un Piano di continuità operativa e di Disaster Recovery, piano redatto sulla base di un dettagliato studio di fattibilità tecnica, **sul quale va obbligatoriamente acquisito il parere di DigitPA.**

Il Piano di Continuità Operativa va aggiornato almeno ogni due anni.

Il Piano di Disaster Recovery, parte integrante del primo, va aggiornato con cadenza almeno annuale, ed entro il 31 dicembre di ogni anno, va inviato (la versione aggiornata) al DigitPA.

per continuità operativa s'intende l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale. Essa comprende sia gli aspetti strettamente organizzativi, logistici e comunicativi (che permettono la prosecuzione delle funzionalità di un'organizzazione) sia la continuità tecnologica, ossia dell'infrastruttura informatica e telecomunicativa (disaster recovery appunto).

- In particolare:
- lo Studio di Fattibilità Tecnica - SFT (comma 4), sul quale deve essere obbligatoriamente richiesto il parere dell'Agenzia per l'Italia Digitale, l'Autorità istituita dalla L. 7 agosto 2012, 134, deve essere sottoposto a visto entro il 30 ottobre 2012;
- la predisposizione del Piano di Continuità Operativa (comma 3, punto a), inclusivo del Piano di Disaster Recovery (comma 3, punto b) e adozione di misure tecniche e organizzative per far fronte agli eventi critici, entro il 31 dicembre 2012.

A tale proposito, data la complessità della materia e i tempi ristretti è indispensabile ricorrere a società specializzate, sia per la redazione dello studio di fattibilità, sia dei piani di disaster recovery e continuità operativa, anche perché, mancando la necessaria esperienza, si correrebbe il rischio di non ottenere il visto da parte di Digit-PA. La proposta allegata, oltre alla redazione dei suddetti documenti, prevede anche un cloud (spazio dedicato alla copie di sicurezza), con sufficienti garanzie di sicurezza, così come richieste dalla Digit-PA nelle recenti linee guida.

Ovviamente, una volta acquisito il visto e redatti i piani, sarà cura dello scrivente provvedere ai conseguenti provvedimenti tecnico-operativi ed organizzativi per la messa in opera di quanto previsto dai suddetti.

Distinti saluti.



IL RESPONSABILE DEL CED

Dott. Nicola Pagano



DigitPA

**LINEE GUIDA PER IL DISASTER RECOVERY DELLE
PUBBLICHE AMMINISTRAZIONI**
*ai sensi del comma 3, lettera b) dell'art. 50-bis del
DLgs. N. 82/2005 e s.m.i.*

2 LE NOVITÀ INTRODOTTE DAL NUOVO CODICE DELL'AMMINISTRAZIONE DIGITALE: RUOLI E RESPONSABILITÀ

2.1 Premessa – Gli obblighi e adempimenti già previsti nel DLgs. 196/2003 e s.m.i.

Il DLgs. 196/2003, contenente le disposizioni del "Codice in materia di Protezione dei dati personali", prevede importanti adempimenti in capo alle Pubbliche Amministrazioni che nell'ambito delle rispettive attività istituzionali si avvalgono di sistemi informativi e gestiscono con strumenti elettronici dati che devono essere protetti adeguatamente sia al fine di evitare accessi non autorizzati e trattamenti illeciti sia per ridurre al minimo, mediante l'adozione di adeguate misure, i rischi di distruzione e perdita.

Si osserva, infatti, che l'articolo 31 del richiamato Decreto prevede: "I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

All'articolo 34 il Decreto richiamato prevede altresì che: "Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato [B], le seguenti misure minime:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

L'allegato B al citato Decreto impone alle Amministrazioni, fra gli altri:

- (regola 19.3) la necessità di descrivere i principali eventi potenzialmente dannosi per la sicurezza dei dati e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati;
- (regola 19.4) l'importanza di individuare le misure in essere e da adottare per contrastare i rischi individuati;
- (regola 19.5) l'importanza di individuare le procedure adottate per il salvataggio e il ripristino dei dati, ovvero per assicurare le procedure di re-installazione delle copie dei dati e prevedere test efficaci delle procedure di salvataggio e ripristino dei dati adottate.

2.2 Le novità in materia di digitalizzazione dell'azione amministrativa e di Continuità operativa

Il Codice dell'Amministrazione digitale (così come aggiornato alla luce del DLgs. n. 235/2010), rafforza ulteriormente il quadro giuridico descritto e l'obbligo delle Pubbliche Amministrazioni di assicurare oltreché la corretta formazione, raccolta e conservazione di dati, la costante operatività dei sistemi informativi quale presupposto fondamentale per la qualità e costante fruibilità dei dati, delle informazioni e dei servizi che le stesse PA rendono ai cittadini e alle imprese.

L'art. 2 del CAD aggiornato (che attiene alle "Finalità e all'ambito di applicazione") precisa che: "Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione".

L'art. 12 del CAD aggiornato (contenente "Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa") confermando le finalità richiamate nel citato articolo 2 prevede che: "Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, nonché per la garanzia dei diritti dei cittadini e delle imprese".

La crescente complessità delle attività legate alla Pubblica Amministrazione, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio, quali quelli determinati da un attacco di tipo terroristico o anche solamente malevolo, così come gli inconvenienti di natura tecnica, che possono portare all'interruzione totale dei servizi istituzionali anche per lunghi periodi, evidenziano l'esigenza che le amministrazioni aggiornino il livello di predisposizione a questi potenziali fermi della propria operatività.

In questa direzione, è quindi necessario che le pubbliche amministrazioni adeguino e rafforzino le strategie in tema di sicurezza in modo da garantire la continuità di funzionamento dei sistemi informativi attraverso i quali le stesse Pubbliche Amministrazioni assicurano lo svolgimento dei rispettivi compiti istituzionali e l'erogazione dei servizi all'utenza.

Le pubbliche amministrazioni devono quindi dotarsi nella gestione corrente dei propri servizi ICT, di strumenti, accorgimenti e procedure per assicurare la Continuità Operativa (CO), per poter far fronte a incidenti di ampia portata o a eventi imprevisibili che possono comportare l'indisponibilità del proprio Sistema Informativo, al fine di evitare fermi o gravi interruzioni della propria operatività con impatti negativi o disservizi nei procedimenti svolti e nei servizi erogati all'utenza. L'attuazione della continuità operativa risulta quindi un adempimento inderogabile, tenuto anche conto delle disposizioni in tema di dematerializzazione e conservazione, quali, in particolare, gli articoli di seguito riportati:

Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni

1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.

Art. 43. Riproduzione e conservazione dei documenti

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.

3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71.

4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42.

Art. 44. Requisiti per la conservazione dei documenti informatici

1. Il sistema di conservazione dei documenti informatici assicura:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) l'integrità del documento;

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originali;

d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.

1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

In questo scenario generale 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 e i compiti che spettano alle Pubbliche Amministrazioni, a DigitPA e al Ministro per la pubblica amministrazione e l'innovazione, ai fini dell'attuazione della continuità operativa:

1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le p.p.a. dispongono i

piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio e 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 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. 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.

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 DigitPA.

Nell'articolo 2 dello stesso CAD, così come innovato dal citato DLgs. 235/2010, in merito alle finalità e all'ambito di applicazione si prevede peraltro quanto segue:

“Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.

2. Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo

1, comma 5, della legge 30 dicembre 2004, n. 311 (...)

5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conforme al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

Tale aspetto diviene interrogabile anche ai fini dell'attuazione della digitalizzazione e per la corretta gestione del sistema di conservazione; l'attuazione degli adempimenti imposti dal CAD (e dalle connesse regole tecniche, previste per i vari ambiti e a cui si rinvia) tende cioè a creare un circolo "virtuoso", schematicamente descritto nella figura seguente:

ESEMPLIFICAZIONE DEL CIRCUITO VIRTUOSO DEL CAD E DEL COLLEGAMENTO FRA GLI ADEMPIMENTI IMPOSTI IN TEMI DI DIGITALIZZAZIONE, GESTIONE DOCUMENTALE, ATTUAZIONE DELLA CONTINUITÀ OPERATIVA, GARANZIA DELLA SICUREZZA DEI DATI, SISTEMI E INFRASTRUTTURE

SERVIZI DELLE PP.AA. EROGATI ATTRAVERSO SISTEMI INFORMATIVI
(Dati, archivi; applicazioni; infrastrutture hw, sw e di rete)

CONSERVAZIONE: ATTUAZIONE DEI PRINCIPI DI GESTIONE DOCUMENTALE: REGOLE TECNICHE DEL CAD per la digitalizzazione e dematerializzazione; (formazione, gestione e trasmissione telematica)

RAZIONALIZZAZIONE alla LUCE DELL'ATTUAZIONE DELLA DIGITALIZZAZIONE NELLA GESTIONE DEI S.I.
(archivi; dati; applicazioni; infrastrutture hw e sw; reti)

Art. 50 bis del CAD: ATTUAZIONE CONTINUITÀ OPERATIVA E DR secondo LINEE GUIDA (a fini della costante fruibilità dei dati, archivi e applicazioni e quindi del mantenimento dell'operatività dei sistemi informativi delle pp.aa. anche a fronte di situazioni di emergenza/disastro)

Art. 51 del CAD: i Sistemi Informativi vanno gestiti nel rispetto delle REGOLE TECNICHE PER LA SICUREZZA DEI DATI, DEI SISTEMI E DELLE INFRASTRUTTURE (che descrive anche le politiche di backup e riavvio per lo specifico tema alle LG su CO/DR)

2.3 Rapporti tra Stato, Regioni, Province autonome ed enti locali

Ai fini dell'applicazione di quanto previsto dal provvedimento normativo in commento, in relazione alle tematiche della continuità ed ai conseguenti obblighi posti in carico a DigitPA, meritano particolare attenzione le novità introdotte in materia di rapporti tra Stato ed enti locali. Ai sensi dell'art.14 del CAD (come novellato dal DLgs. 235/2010) "lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime", si affida alle Regioni ed alle Province autonome un ruolo di guida e coordinamento dell'azione di digitalizzazione dell'azione amministrativa svolta a livello locale; a tal fine, le Regioni, le Province autonome e gli enti locali adottano le tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese (art. 14, co.2bis e 3bis).

Dal combinato disposto dei commi richiamati discende l'obbligo per amministrazioni centrali, regionali, provinciali e comunali di dare attuazione a quanto previsto dall'art'50-bis del nuovo CAD.

2.4 Ruoli e responsabilità per la realizzazione dei Piani di CO e DR

Il quadro normativo richiamato rafforza, quindi, l'importanza dell'adozione, da parte delle Pubbliche Amministrazioni di soluzioni organizzative e tecniche dirette a garantire la continuità operativa dei sistemi Informativi ed affidata:

- **a DigitPA il compito di:**
 - definire, sentito il Garante per la protezione dei dati personali, le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche;
 - verificare annualmente il costante aggiornamento dei Piani di DR delle amministrazioni interessate;
 - informare annualmente il Ministro per la pubblica amministrazione e l'innovazione;
 - esprimere pareri sugli studi di fattibilità che le amministrazioni predispongono e sulla base dei quali provvederanno a definire sia il piano di continuità operativa che il piano di DR.
- **alle Amministrazioni il compito di definire in prima battuta gli studi di fattibilità e sulla base di detti studi - entro quindici mesi dall'entrata in vigore del DLgs 235/2010 - i piani di emergenza, continuità operativa e Disaster Recover.**
- **al Ministro per la pubblica Amministrazione e l'innovazione il compito di:**
 - assicurare l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni;
 - informare con cadenza annuale Il Parlamento.
- **alle Regioni ed alle Province autonome il compito di:**
 - avviare al proprio interno il medesimo percorso di attuazione dell'art.50-bis del CAD;
 - promuovere le iniziative necessarie a generare la consapevolezza sulle specifiche necessità di CO e DR, all'interno degli enti territoriali minori, anche facilitando il percorso di realizzazione da parte delle singole realtà;
 - diffondere le presenti linee guida, quale strumento di agevolazione per la definizione e l'adozione dei piani di CO e DR da parte degli enti territoriali minori.

Le Amministrazioni sono chiamate, quindi, a elaborare studi di fattibilità:

- valutando il proprio contesto tecnico operativo di riferimento;
- verificando l'importanza dei dati rispetto ai procedimenti amministrativi svolti e/o ai servizi erogati verso l'utenza e il cittadino;
- svolgendo attività di Business Impact Analysis (BIA), al fine quindi di verificare i rischi e possibili impatti che si determinano su procedimenti e servizi erogati, a fronte di situazioni di indisponibilità prolungata o di disastro e valutare le soluzioni possibili per mitigare o evitare le situazioni di rischio;
- predisponendo, arricchendo e monitorando periodicamente le misure minime e le politiche di sicurezza e gli accorgimenti organizzativi e tecnici per far fronte a eventi critici o disastrosi (attraverso piani di Continuità Operativa e piani di Disaster Recovery)

Le Pubbliche Amministrazioni sono chiamate sia a definire le soluzioni per affrontare le conseguenze di eventi critici che possano pregiudicare la sicurezza dei dati e la continuità di funzionamento dei Sistemi Informativi, sia a tenere costantemente sotto controllo le soluzioni adottate attraverso un'adeguata pianificazione, verifica e test delle misure e accorgimenti adottati.



DigitPA

L'attuazione delle norme richiamate ed in particolare gli adempimenti previsti dall'art. 50 bis per l'attuazione della continuità operativa ICT, si ritiene possano anche comportare, come del resto è nello spirito del CAD, una verifica e revisione del modo di operare delle Amministrazioni e lo stimolo ad una maggiore razionalizzazione e digitalizzazione dei servizi ICT.

Tale esigenza trova particolare riscontro per una corretta gestione del sistema di conservazione di cui agli art. 44 e 44 bis del CAD.

Al riguardo, per affrontare l'attuazione delle novità richiamate, le Pubbliche Amministrazioni possono far riferimento per gli adempimenti di competenza e per quello che attiene alla predisposizione di studi di fattibilità, sia alle presenti linee guida sia alle Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti per la Pubblica Amministrazione - Manuale applicativo 8, "Analisi di fattibilità per l'acquisizione delle forniture ICT" vers. 1.3 del 4.2.2009.

Le Amministrazioni devono, una volta acquisito il parere obbligatorio di DigitPA sullo studio di fattibilità tecnica, definire conseguentemente i Piani per descrivere le misure organizzative e tecniche di cui intendono dotarsi per garantire la continuità operativa e il Disaster Recovery.

Inoltre, per consentire a DigitPA di verificare annualmente il costante aggiornamento dei piani di Disaster recovery delle Amministrazioni e informare il Ministro per la pubblica amministrazione e l'innovazione, le Amministrazioni dovranno inviare a DigitPA i piani di Disaster Recovery, e devono verificare la funzionalità del piano di continuità operativa con cadenza biennale.

Come si avrà modo di evidenziare nel prosieguo spetta più in generale alle Amministrazioni curare la gestione e manutenzione della soluzione di CO/DR adottata provvedendo a verificare costantemente l'adeguatezza della stessa, attraverso attività periodiche di verifica e test e a garantire il costante aggiornamento della soluzione stessa.

Ai fini delle attività di verifica attribuite a DigitPA si ritiene opportuno che le Amministrazioni invino successivamente anche informazioni in merito alle verifiche periodiche effettuate e agli esiti di dette verifiche.

L'omogeneità delle soluzioni indicate in questi piani è assicurata dal Ministro per la pubblica amministrazione e l'innovazione, che ne informa con cadenza almeno annuale il Parlamento.

Nella figura seguente si riporta, in forma schematica, la descrizione del procedimento desumibile dalla norma citata, ipotizzando anche per ciascuna fase, obiettivi e risultati attesi per ciascuno degli "attori" coinvolti nell'attuazione degli adempimenti previsti dal richiamato art. 50 bis.

Ritenuta l'opportunità di aderire a questa proposta, in quanto garantisce la totale conformità alle norme sopracitate e un livello di assistenza tecnica continua, favorendo economie di scala.

Considerato che tale proposta **comporta adesione formale** e approvazione esplicita delle allegate condizioni di adesione al servizio erogato attraverso la **società consorziata Asmenet Campania scarl.**

Richiamato il Codice in materia di protezione dei dati personali di cui al Decreto Legislativo 30 giugno 2003, n° 196.

Richiamato il Decreto legislativo 30 dicembre 2010, n° 235 (G. U. 10/01/2011, n° 6).

Acquisito il parere favorevole espresso dal responsabile del servizio interessato ai sensi dell'art. 49 - del Decreto Legislativo 18 agosto 2000, n° 267.

Con Voti unanimi favorevoli espressi per alzata di mano dai convenuti.

Delibera

- **la premessa** costituisce parte integrante della presente, per cui si intende qui ripetuta e trascritta.

- **aderire** al Servizio START + BRD + MAN - AsmeCloud per la **Continuità Operativa** e il **Disaster Recovery**, secondo le modalità previste nella documentazione tecnica, che **allegata** alla presente ne forma parte integrante e sostanziale.

- **dare mandato** al Responsabile dell'Area Finanziaria di prevedere la dovuta copertura finanziaria nell'importo di **€uro 1.694,00** - Iva inclusa come per legge, nel bilancio annuale 2012, in sede di assestamento generale dello stesso e, l'importo di **€uro 500,00** nel bilancio pluriennale per gli anni seguenti, con attribuzione al Responsabile dell'Area Amministrativa.

- **dare mandato** altresì, al Responsabile dell'Area Amministrativa e al Responsabile del Servizio CED, di provvedere ad adottare tutti gli atti necessari e susseguenti, ivi compreso l'impegno di spesa e susseguente liquidazione, secondo i tempi stabiliti, relativi alla realizzazione dell' intervento, rispettivamente per la parte amministrativa e tecnico-operativa.

- **pubblicare** il presente provvedimento all'Albo **On - Line** del Comune.

- **trasmettere** la presente, in elenco, ai sig.ri Capigruppo Consiliari, ai sensi dell'art. 125 - del Decreto Legislativo 18/08/2000, n° 267 (TUEL).

- **dichiarare** la presente, con separata votazione palese ed a voti unanimi, immediatamente eseguibile ai sensi e per gli effetti dell'art. 134 - comma 4° - del Decreto Legislativo 18/08/2000, n° 267 (TUEL), stante l'urgenza di provvedere. -

Letto, approvato e sottoscritto
Sindaco
F.to Geom. Franco Martino

IL SEGRETARIO COMUNALE
F.to Dr. Fernando Antico

L'ASSESSORE
F.to Sig. Luigi Mastrantuono



PUBBLICAZIONE

La presente deliberazione, ai sensi dell'art. 124 - del T. U. E. L. n° 267 / 2000, VIENE affissa all'Albo Pretorio Comunale per quindici giorni consecutivi a decorrere dal 24 GEN. 2013;

E' stata dichiarata immediatamente eseguibile (art. 134, comma 4°, del T. U. E. L. n° 267 / 2000);

E' stata trasmessa con lettera n° 0354, in data 24 GEN. 2013, ai sigg. Capigruppo Consiliari, come prescritto dall'art. 125, del T. U. E. L. n° 267 / 2000;

Dalla Residenza Comunale, 24 GEN. 2013



IL SEGRETARIO COMUNALE
F.to Dr. Fernando Antico

E' copia conforme all'originale per uso amministrativo e di ufficio.

Dalla Residenza Comunale, 24 GEN. 2013



IL SEGRETARIO COMUNALE
Dr. Fernando Antico

ESECUTIVITA'

Il sottoscritto Segretario Comunale, visti gli Atti d'Ufficio,

ATTESTA

che la presente deliberazione E' STATA AFFISSA all'Albo Pretorio Comunale per quindici giorni consecutivi a decorrere dal 24 GEN. 2013, come prescritto dall'art. 124, comma 1°, del T. U. E. L. n° 267 / 2000), ed è divenuta esecutiva decorsi 10 giorni dalla pubblicazione (art. 134, comma 3°, del T. U. E. L. n° 267 / 2000). -

IL SEGRETARIO COMUNALE
Dr. Fernando Antico

Dalla Residenza Comunale, _____