Piano di Continuità Operativa

- **FINALITÀ E AMBITO DI APPLICAZIONE**: dovrebbero esser indicati i servizi da recuperare e le priorità di recupero, i tempi entro i quali i servizi devono essere recuperati (RTO), i livelli di recupero dei dati necessario per ogni servizio (RPO), le condizioni che portano a invocare il piano
- **RUOLI E RESPONSABILITÀ**: dovrebbero essere indicati i ruoli/responsabilita' delle persone e del team che sono coinvolti, in termini di processo decisionale e di livello di autorità durante e dopo un'emergenza
- **MODALITÀ DI ATTIVAZIONE, GESTIONE E MANUTENZIONE DEL PCO**: dovrebbero essere indicate le modalità per mobilitare le persone e i team interessati, la localizzazione dei punti di ritrovo dei team interessati, le circostanze in cui l'organizzazione ritiene che l'attivazione del PCO non sia necessaria, le modalità di gestione, manutenzione e verifica e test del PCO, **il piano di disaster recovery**, le modalità di rientro dall'emergenza

Piano di Disaster Recovery

- FINALITÀ E I CONTENUTI DEL PIANO DI DR
- DESCRIZIONE DELLA SOLUZIONE DI DR
- OBIETTIVI DEL PIANO DI DR
- INFORMAZIONI RELATIVE AL PIANO DI DR
- CLAUSOLE E DIRETTIVE APPLICABILI
- PERIMETRO DI RIFERIMENTO DEL PIANO
- ORGANIZZAZIONE E PERSONALE
- POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI
- FASI DELLA SOLUZIONE DI DISASTER RECOVERY
- GESTIONE DEL PIANO
- COLLEGAMENTI / EVENTUALI INTERAZIONI CON GLI ALTRI DELIVERABLE CONTRATTUALI
- PROCEDURE DI TEST

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.

BREVE GUIDA ALLA LETTURA

Il documento è interamente correlato ai contenuti e redatto ai sensi del comma 3, lettera b) dell'art. 50-bis del DLgs. N. 82/2005 e s.m.i., "Continuità operativa", come modificato dal DLgs. 235/10.
Preliminarmente, si premette che, ancorché l'art. 50-bis preveda la produzione, a cura di DigitPA, delle "linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni", di cui questo documento è l'attuazione, i contenuti del documento sono stati estesi anche a:

- indicazioni nel merito dei contenuti e della produzione del piano di continuità operativa;
- indicazioni e schemi di massima dello studio di fattibilità tecnica,

per fornire alle Amministrazioni gli elementi necessari al completo adempimento ai dispositivi dell'articolo.

I contenuti delle Linee Guida sono i seguenti:

- il capitolo 1 definisce gli obiettivi e gli scenari della continuità operativa e del Disaster Recovery nell'ambito delle pubbliche amministrazioni e le finalità delle Linee Guida;
- il capitolo 2 descrive le novità introdotte dal nuovo codice della amministrazione digitale, con riferimento specifico alla tematica della continuità operativa, illustrando i ruoli e le responsabilità assegnate dal nuovo CAD alle pubbliche amministrazioni e alla stessa DigitPA;
- il capitolo 3 riporta informazioni sintetiche sui principali standard internazionali di riferimento attinenti al campo specifico della continuità operativa e del Disaster Recovery e alle aree correlate della sicurezza ICT e della gestione dei servizi informatici;
- il capitolo 4 costituisce una guida sulle modalità con cui affrontare il problema della continuità operativa sotto l'aspetto organizzativo. In particolare vengono fornite indicazioni su come impostare il progetto affinché l'obiettivo della continuità dei servizi possa essere raggiunto efficacemente e mantenuto nel tempo al variare delle condizioni al contorno;
- il capitolo 5 illustra metodi con cui è possibile affrontare il tema della continuità operativa e propone un percorso di autovalutazione dei requisiti di continuità cui le amministrazioni dovranno sottoporsi per la successiva identificazione delle soluzioni tecnologiche idonee a garantire la continuità nella erogazione dei servizi anche a fronte di disastri che compromettano il funzionamento di parte o dell'intera infrastruttura ICT;
- il capitolo 6 analizza la continuità operativa sotto il profilo delle opzioni e dei vincoli previsti dalla normativa vigente ed illustra, anche con esempi, le soluzioni contrattuali che possono essere intraprese dalla Pubblica Amministrazione. Sono presenti anche alcuni spunti per la definizione di forme associative tra amministrazioni che consentono il contenimento dei costi (accordi di mutuo soccorso, convenzioni, consorzi, centri di backup comuni, ecc.);
- il capitolo 7 illustra il modello di riferimento di massima che dovrà essere utilizzato per la compilazione dello studio di fattibilità tecnica che le amministrazioni pubbliche devono sottoporre a DigitPA per il parere obbligatorio previsto dal comma 4 dell'art. 50-bis del CAD nonché indicazioni di massima dei contenuti dei Piani di CO e di DR;
- il capitolo 8 presenta la tematica della protezione delle infrastrutture critiche, oggetto di recenti interventi normativi a livello europeo e nazionale;
- il capitolo 9 riporta le conclusioni e una sintesi dei contenuti ed obiettivi del documento.

Il documento è completato da alcune appendici in cui sono proposti schemi di documenti di analisi e pianificazione, nonché elementi utili ai fini contrattuali quali i requisiti dei siti di DR ed esempi di livelli di servizio.

Percorso minimo di lettura
Al fine di semplificare l'utilizzo del documento si riporta nel seguito un percorso minimo di lettura che consente di acquisire gli strumenti conoscitivi essenziali per ottemperare agli obblighi imposti dall'art.50 bis del CAD.

Capitolo 1	OBIETTIVI E SCENARI DELLA CONTINUITÀ OPERATIVA DELLE PUBBLICHE AMMINISTRAZIONI.
Capitolo 2	§ 2.2 - Le novità in materia di digitalizzazione dell'azione amministrativa e di Continuità operativa. § 2.4 - Ruoli e responsabilità per la realizzazione dei Piani di CO e DR.
Capitolo 4	§ 4.1 - Coinvolgimento dei vertici dell'amministrazione e ruolo della struttura di gestione. § 4.2 - Il Comitato di gestione della crisi. § 4.6 - Indicazioni per il collaudo e per i test di verifica periodica dell'adeguatezza della soluzione.
Capitolo 5	§ 5.1 - Determinazione delle esigenze di continuità e delle soluzioni. § 5.2 - Strumenti per l'autovalutazione. § 5.4 - Lo strumento di supporto per l'autovalutazione.
Capitolo 6	§ 6.2 - La realizzazione di soluzioni di continuità operativa.
Capitolo 7	LO STUDIO DI FATTIBILITÀ TECNICA E I PIANI PER LA CO E IL DR DELLE PA.
APPENDICI	APPENDICE C: STRUMENTO DI SUPPORTO PER L'AUTOVALUTAZIONE APPENDICE D: POSSIBILI REQUISITI DEL SITO DI DR. APPENDICE E: ESEMPI DI LIVELLI DI SERVIZIO.

Il documento è stato redatto e curato dal "Gruppo di lavoro DigitPA per la Continuità Operativa e le Infrastrutture critiche", dal Prof Antonio Orlandi (Coordinatore), dalla D.ssa Cristina Di Domenico, dal Dott. Giovanni Rellini Lerz, dal Dott. Gabriele Cicognani e dall'Ing. Alessandro Alessandroni.

Hanno partecipato alle attività del Gruppo di lavoro:

Arma dei Carabinieri – Colonnello Vincenzo Galli, Maggiore Gianluigi Me
Banca di Italia – Ing. Guido Pagani, D.ssa Isabella Stefanangeli, Ing. Stefano Simeoni
CISIS – Dott. Andrea Nicolini
CONSIP – Ing. Gaetano Santucci, Dott. Massimo Fedeli
INAIL – Dott. Luigi Gugliotti, Ing. Augusto Beccari
Informatica Trentina (Provincia Autonoma di Trento) – Dott. Pierluigi Sartori
Innovapuglia (Regione Puglia) – Ing. Vitantonio Martino
INPDAP – Ing. Paolo Moncelsi
INPS – Dott. Massimiliano D'Angelo, Ing. Giovanni Ceccarelli
MEF – Ing. Raffaele Visciano
Regione Emilia Romagna – Dott. Alessandro Landi
Regione Liguria – Dott. Alfredo Gambino

Glossario delle principali definizioni utilizzate nel documento

Nell'ambito del presente documento si intende per:

- *Allineamento dei dati:* il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;

- *Archivio:* complesso organico dei documenti, dei fascicoli e delle serie archivistiche di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento della propria attività, che si distingue in relazione alle diverse fasi di gestione in: archivio corrente, archivio di deposito e archivio storico (come precisato dalle relative regole tecniche);

- *BIA (Business Impact Analysis*): la metodologia da utilizzare al fine di determinare le conseguenze derivanti dal verificarsi di un evento critico e di valutare l'impatto di tale evento sull'operatività dell'amministrazione, richiamata in appendice A al presente documento;

- *Comitato di gestione della crisi*: la struttura organizzativa definita per la continuità: la struttura con responsabilità e compiti ben definiti, descritta nel capitolo 4, con autonomia decisionale e disponibilità di utilizzare risorse straordinarie, ai fini del governo dell'emergenza, che include il Responsabile della Continuità e non può comunque prescindere dalle attribuzioni previste in capo all'Unità Locale per la Sicurezza (ULS) istituita all'interno di ogni amministrazione per il governo degli aspetti di sicurezza relativi all'adesione al Sistema Pubblico di Connettività;

- *Continuità Operativa/Business Continuity (CO/BC)*: l'insieme delle attività e delle politiche adottate per ottemperare all'obbligo di assicurare la continuità nel funzionamento dell'organizzazione; è parte integrante dei processi e delle politiche di sicurezza di un'organizzazione;

- *Continuità operativa ICT:* la capacità di un organizzazione di adottare, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative, misure di reazione e risposta ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi ICT utilizzati per lo svolgimento delle funzioni istituzionali;

- *Copia dei dati (Data Mirroring):* un processo con cui dati ritenuti critici vengono copiati secondo precise regole e politiche di backup al fine di garantire l'integrità, la custodia e la fruibilità degli archivi, dei dati e delle applicazioni e la possibilità di renderli utilizzabili, ove fosse necessario, procedendo al ripristino degli archivi, dei dati e delle applicazioni presso un sito alternativo a quello primario;

- *Database*: collezione di dati registrati e correlati fra loro;

- *Dato:* rappresentazione oggettiva di un fatto o un evento che consente la sua gestione e trasmissione da parte di un soggetto umano o uno strumento informatico; l'elaborazione dei dati può portare alla conoscenza di un informazione; ai fini della gestione documentale ha rilevanza il concetto di *Metadato*, che attiene all'insieme dei dati associati a un documento informatico o a un fascicolo informatico o a una serie documentale informatica per descriverne il contesto, il contenuto, la struttura nonché permetterne la gestione nel tempo;

- *Dato delle pubbliche amministrazioni:* il dato formato o comunque trattato da una pubblica amministrazione;

- *Digitalizzazione ICT:* il richiamo ai principi del CAD che comportano la dematerializzazione, la formazione, gestione, conservazione e trasmissione dei documenti informatici, che portando le Amministrazioni ad una razionalizzazione e informatizzazione della gestione documentale rafforzano l'importanza di assicurare una corretta attuazione delle politiche di sicurezza e di backup e la predisposizione, gestione e manutenzione di soluzioni di CO/DR ai sensi dell'art. 50 bis del CAD;

- *Disaster recovery (DR)*: nell'ottica dell'art. 50 bis del CAD, l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate;

- *Fruibilità di un dato:* la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

- *Gestione informatica dei documenti*: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;

- *Infrastruttura*: un elemento, un sistema o parte di questo, che contribuisce al mantenimento delle funzioni della società, della salute, della sicurezza e del benessere economico e sociale della popolazione;

- *Infrastruttura Critica*: un'infrastruttura che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo nello Stato, a causa dell'impossibilità di mantenere tali funzioni;

- *Log:* la registrazione cronologica delle operazioni eseguite su di un sistema informatico, e quindi su archivi, per finalità quali ad es.: controllo e verifica degli accesi (access log), registro e tracciatura dei cambiamenti che le transazioni introducono in un Data-base (log di transazioni o log di base dati), analisi delle segnalazioni di errore (error log), produzione di statistiche di esercizio;

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

- *Piano di Disaster Recovery (PDR)*: il Piano che, costituisce parte integrante del Piano di continuità operativa e stabilisce le misure tecniche ed organizzative per garantire il funzionamento dei centri elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione;

- *Piano per la Sicurezza dell'Operatore (PSO):* il Piano che deve identificare i beni dell'infrastruttura critica e le soluzioni in atto o in corso di implementazione per la loro protezione;

- *Politiche di sicurezza:* le regole tecniche e le politiche adottate per garantire l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture, la prevenzione e gestione degli incidenti di sicurezza informatica nonché per assicurare che i documenti informatici siano custoditi e controllati in modo tale da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alla finalità della raccolta;

- *Risk Assessment (RA):* l'analisi per determinare il valore dei rischi di accadimento di un evento che possa interrompere la continuità operativa;

- *RPO: Recovery Point Objective*, indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso;

- *RTO: Recovery Time Objective*, indica il tempo di ripristino del servizio: è la durata di tempo e di un livello di servizio entro il quale un business process ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili;

- *Servizio ICT*: qualunque elemento ICT, processo ICT, sistema ICT o parte di esso, attività svolta mediante ICT, che serva ovvero produca effetti all'interno e/o all'esterno dell'organizzazione e la cui compromissione impatti sullo svolgimento delle funzioni istituzionali delegate;

- *Studio di fattibilità tecnica (SFT)*: lo studio sulla base del quale le Amministrazioni devono adottare il piano di continuità operativa e il piano di Disaster Recovery e su cui va obbligatoriamente acquisito il parere di DigitPA;

- *Strumento di autovalutazione:* lo strumento che si propone nel presente documento, nell'ambito del percorso descritto nel capitolo 5, ai fini della predisposizione degli studi di

fattibilità tecnica e dei piani di CO e DR, per supportare le amministrazioni nell'identificazione delle soluzioni tecnologiche idonee alla continuità operativa, avendo come base di partenza, essenzialmente i "servizi" che l'ente eroga;

- *SPC:* Sistema Pubblico di Connettività (artt. 73 e segg. del DLgs 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" e s.m.i.); è definito come l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.

1 OBIETTIVI E SCENARI DELLA CONTINUITÀ OPERATIVA DELLE PUBBLICHE AMMINISTRAZIONI

L'art. 97 della Costituzione sancisce, tra gli altri, un generale principio organizzativo di carattere programmatico che riguarda l'amministrazione dello Stato nel suo complesso: gli uffici pubblici devono essere organizzati in modo che siano garanti il buon funzionamento e l'imparzialità dell'amministrazione.
Da tale principio consegue per la Pubblica Amministrazione anche l'obbligo di assicurare la continuità dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese; questa affermazione assume particolare significato in considerazione del sempre maggiore utilizzo delle tecnologie ICT per la gestione dei dati e dei processi interni ai singoli enti, il cui impiego deve essere realizzato anche pianificando le necessarie iniziative tese a salvaguardare l'integrità e la disponibilità delle informazioni stesse.
Quando i dati, le informazioni e le applicazioni che li trattano sono parte essenziale ed indispensabile per lo svolgimento delle funzioni istituzionali di un ente/organizzazione, diventano un bene primario cui è necessario garantire salvaguardia e disponibilità; essendo la disponibilità uno dei cardini della sicurezza, unitamente a confidenzialità ed integrità, la disciplina della continuità operativa (nel seguito anche CO) rappresenta parte integrante dei processi e delle politiche di sicurezza di un'organizzazione.
La previsione e l'adozione di misure che garantiscono la disponibilità dei dati, indipendentemente dagli eventi che possono occorrere, rappresentano un dovere per quanti hanno la responsabilità di assicurare l'efficienza della PA in generale ed il buon funzionamento degli uffici pubblici in particolare.
Tutte le azioni che saranno descritte in queste Linee Guida, pertanto, dovranno essere considerate come uno degli adempimenti necessari a completare ed integrare tutte le misure di sicurezza dell'organizzazione medesima e che trovano fondamento anche in altri obblighi normativi (si pensi in particolare al Codice della Privacy, alla normativa sui collaudi, al T.U. sulla sicurezza nel lavoro - DLgs 81/2008 e s.m.i.; al DPCM 01.04.2008, ecc) e nelle Regole tecniche di cui all'art. 51 del Codice dell'Amministrazione Digitale (inerente la "Sicurezza dei dati, dei sistemi e delle infrastrutture"), come evidenziato anche nel successivo par. 2.5.
In quest'ottica anche l'attuazione degli obblighi imposti dal CAD in materia di CO possono costituire un'occasione per sensibilizzare le Amministrazioni verso un percorso complessivo in materia di sicurezza di tutta l'organizzazione, coerentemente con il quadro normativo richiamato, nonché un momento per rivisitare e razionalizzare le risorse dedicate.

In linea generale, la Continuità Operativa è intesa come l'insieme delle attività e delle politiche adottate per ottemperare all'obbligo di assicurare la continuità nel funzionamento dell'organizzazione.
Quest'obbligo finora è stato assolto, a fronte di eventi che hanno avuto un impatto sul regolare funzionamento dell'organizzazione, ricorrendo a soluzioni di emergenza di tipo tradizionale quali: il trasferimento dei servizi presso gli uffici rimasti operativi, l'attivazione di procedure amministrative alternative, l'ausilio di personale aggiuntivo, ecc. Oggi l'impiego di procedure alternative di tipo tradizionale è quasi sempre insufficiente a garantire la continuità dei servizi, atteso il diffuso utilizzo delle tecnologie informatiche. Anche qualora il procedimento amministrativo appaia "non informatizzato", una fase del suo procedimento è stata assolta mediante applicazioni informatiche; inconvenienti di natura tecnica, pertanto, possono condizionare il

normale svolgimento dei processi tradizionali, fino a comportare il blocco delle attività istituzionali anche per lunghi periodi.
In particolare il processo di dematerializzazione promosso dal CAD, che con le sue disposizioni ha trasformato da ordinatoria a perentoria l'azione di eliminazione della carta, comporta un incremento della criticità dei sistemi informatici che non possono più contare su un backup basato sulla documentazione cartacea.

Da quanto detto consegue che la continuità dei servizi informatici rappresenta un impegno inderogabile per la Pubblica Amministrazione che dovrà operare in modo da limitare al massimo gli effetti negativi di possibili fermi prolungati dei servizi ICT. A titolo esemplificativo, la compromissione della continuità di un sistema informatico, può essere conseguenza di:

- errori/malfunzionamenti dei processi (il processo organizzativo che usa il servizio ICT non ha funzionato come avrebbe dovuto per errori materiali, errori nell'applicazione di norme ovvero per il verificarsi di circostanze non adeguatamente previste dalle stesse);
- malfunzionamento dei sistemi, delle applicazioni e delle infrastrutture;
- attacchi o eventi naturali di tipo accidentale;
- disastri.

Fra le conseguenze di eventi che possono colpire un organizzazione causando il blocco del Sistema Informatico, si definisce "disastro", l'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'organizzazione.
Al riguardo, la Continuità operativa comprende fra le attività e soluzioni possibili, il "Disaster Recovery", che più propriamente attiene agli accorgimenti organizzativi e alle soluzioni tecniche, organizzative e procedurali adottate per garantire il **ripristino** dello stato del Sistema Informatico (o di parte di esso), per riportarlo alle condizioni di funzionamento e di operatività antecedenti a un evento disastroso.

Le espressioni *Disaster Recovery* e *business continuity* sono usate con varie accezioni e, talvolta, come sinonimi.

Qualche esempio potrà chiarire meglio queste espressioni. Un problema hardware è un evento ordinario che viene di solito gestito secondo quanto previsto dalle procedure di manutenzione con livelli di servizio commisurati all'impiego dell'apparato. Un guasto hardware può causare una discontinuità operativa ma, quando il periodo di interruzione rientra nei parametri di qualità del servizio, tale evento viene considerato normale e non provoca l'innesco del piano di continuità operativa. Può accadere, però, che per motivi imprevisti (ad esempio per irreperibilità di una parte di ricambio), il periodo di interruzione sia superiore a quello accettabile secondo i parametri di qualità del servizio. In tale evenienza, anche se la causa del problema è un evento ordinario, è opportuno gestire la circostanza particolare secondo le modalità descritte nel presente documento, ossia con i metodi e le tecniche della continuità operativa. Analogamente, se un problema di sicurezza determina un'interruzione del servizio di durata eccessiva, può essere opportuno avviare le procedure di continuità operativa per garantire che l'interruzione rimanga entro limiti tollerabili.
Occorre osservare che tra gli eventi elencati sussiste una differenza che condiziona alquanto gli approcci alla continuità operativa.
Gli eventi di tipo calamitoso (incendi, allagamenti, ecc.) si manifestano subito nella loro gravità e dunque comportano senz'altro la partenza del piano di continuità operativa.
I problemi di qualità e di sicurezza si manifestano invece inizialmente come problemi ordinari e solo a seguito di ripetuti insuccessi delle procedure abituali di recupero assumono la consistenza dei problemi di continuità operativa. Infatti la gravità del problema può aumentare progressivamente

nel tempo senza che sia possibile determinare in anticipo il livello di criticità che assumerà l'evento. Ciò comporta la necessità di stabilire, volta per volta, se sia il caso o meno di avviare le procedure di continuità operativa e questa decisione sarà tanto più critica quanto maggiori saranno i costi per l'avvio del piano di continuità operativa ed il rientro alla normalità.

Nel seguito del documento la gestione della continuità del servizio sarà associata alle conseguenze di eventi di natura eccezionale che impattano un'organizzazione.

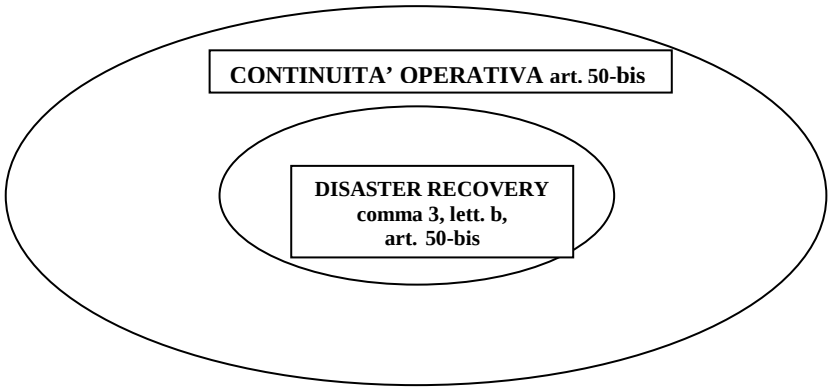
Per continuità operativa ICT - ai sensi e per le finalità di queste linee guida - si intende la capacità di un organizzazione di adottare, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative, misure di reazione e risposta ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi ICT utilizzati per lo svolgimento delle funzioni istituzionali.
In tal senso la continuità operativa ICT deve, quindi, garantire la protezione dalle potenziali criticità delle funzionalità informatiche, tenendo conto delle risorse umane, strutturali, tecnologiche riferibili all'infrastruttura informatica, stabilendo le idonee misure preventive e correttive nel rispetto dei livelli prestazionali riconosciuti.
A tal fine, il perimetro di competenza della continuità operativa ICT deve comprendere almeno:

- le applicazioni informatiche e i dati del sistema informativo indispensabili all'erogazione dei servizi e allo svolgimento delle attività (informatiche e non);
- le infrastrutture fisiche e logiche che ospitano sistemi di elaborazione;
- i dispositivi di elaborazione hardware e software che permettono la funzionalità delle applicazioni realizzanti i servizi dell'amministrazione;
- le componenti di connettività locale e/o remota/geografica;
- ciò che serve per consentire lo svolgimento delle attività del personale informatico, sia interno all'amministrazione, sia, se presente, esterno, ma correlato al sistema informativo stesso;
- le modalità di comunicazione ed informazione al personale utilizzatore del sistema informativo all'interno dell'amministrazione e ai fruitori esterni dei servizi del sistema informativo dell'amministrazione, siano essi cittadini, imprese, altre amministrazioni;
- le misure per garantire la disponibilità dei sistemi di continuità elettrica (UPS e gruppi elettrogeni) e più in generale la continuità di funzionamento del sistema informativo;
- la gestione dei posti di lavoro informatizzati dell'amministrazione;
- i servizi previsti per l'attuazione del C.A.D. (fra cui ad es. la PEC; la firma Digitale ecc.)

Per quanto riguarda i posti di lavoro informatizzati (PDL), agli effetti della soluzione di continuità operativa è importante, tenuto conto delle caratteristiche del sistema informativo e delle applicazioni informatiche di cui deve essere garantito il funzionamento, considerare:

- il numero minimo di PDL che possa garantire la funzionalità dell'ufficio o della sede dove risiedono i PDL;
- la disponibilità di PDL di emergenza presso altri uffici o presso altre sedi dell'amministrazione;
- la disponibilità di dispositivi (workstation) alternativi, quali portatili, nello stesso ufficio o presso sedi diverse dell'amministrazione;
- la disponibilità di connettività alternativa (collegamenti ridondati, collegamenti via UMTS);
- la disponibilità di sistemi di continuità elettrica (UPS e gruppi elettrogeni).

Nell'ottica dell'art. 50 bis del CAD, si definisce più propriamente, "Disaster Recovery" l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate.



Nel presente documento verrà anche proposto un percorso di autovalutazione cui le amministrazioni dovranno sottoporsi per la successiva identificazione delle soluzioni tecnologiche idonee alla continuità operativa, avendo come base di partenza, essenzialmente i "servizi" che l'ente eroga.
Con tale espressione si vuole ricomprendere: qualunque elemento ICT, processo ICT, sistema ICT o parte di esso, attività svolta mediante ICT, che serva ovvero produca effetti all'interno e/o all'esterno dell'organizzazione e la cui compromissione impatti sullo svolgimento delle funzioni istituzionali delegate.

Obiettivo quindi delle presenti Linee guida è quello di fornire degli strumenti per ottemperare agli obblighi derivanti dall'art 50-bis del CAD, obblighi che saranno più diffusamente illustrati nel successivo Capitolo 2.

L'art. 50-bis, al comma 3, lett. b, prevede la produzione, a cura di DigitPA, delle linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni, di cui questo documento è l'attuazione. Il documento contiene anche:

- indicazioni nel merito dei contenuti e della produzione del piano di continuità operativa;
- indicazioni e schemi di massima dello studio di fattibilità tecnica,

per fornire alle Amministrazioni gli elementi necessari al completo adempimento ai dispositivi dell'articolo.

Il documento si propone, pertanto, di essere utilmente adottato da tutte quelle Amministrazioni che:

- già si sono dotate di piani di CO e di DR e che potranno, mediante lo strumento di autovalutazione, verificare la corrispondenza delle soluzioni già adottate con quelle presentate nel seguito come riferimento omogeneo per tutta la PA;
- devono ancora dotarsi di piani di CO e DR e possono trovare un valido orientamento per ottemperare agli obblighi imposti dall'art.50-bis del CAD.

In forza di detto articolo, infatti, è prevista anche la verifica annuale del costante aggiornamento dei piani di DR, con l'obiettivo di assicurare l'omogeneità delle soluzioni di continuità operativa; a tal fine, il testo normativo affida al Ministro per la pubblica Amministrazione e l'innovazione anche il compito di informare al riguardo, con cadenza annuale, il Parlamento.

Compito di DigitPA sarà anche quello di aggiornare le presenti Linee Guida secondo le più innovative soluzioni tecnologiche che dovessero rendersi disponibili, mettendo a disposizione della PA - in tal modo - uno strumento dinamico in grado di fornire un supporto operativo sempre aggiornato all'evoluzione tecnologica.

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:*

a. *autenticazione informatica;*
b. *adozione di procedure di gestione delle credenziali di autenticazione;*
c. *utilizzazione di un sistema di autorizzazione;*
d. *aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;*
e. *protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;*
f. *adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;*
g. *tenuta di un aggiornato documento programmatico sulla sicurezza;*
h. *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 comunicazione 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 imprevisti 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 ì dati di registrazione e di classificazione originari;
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.

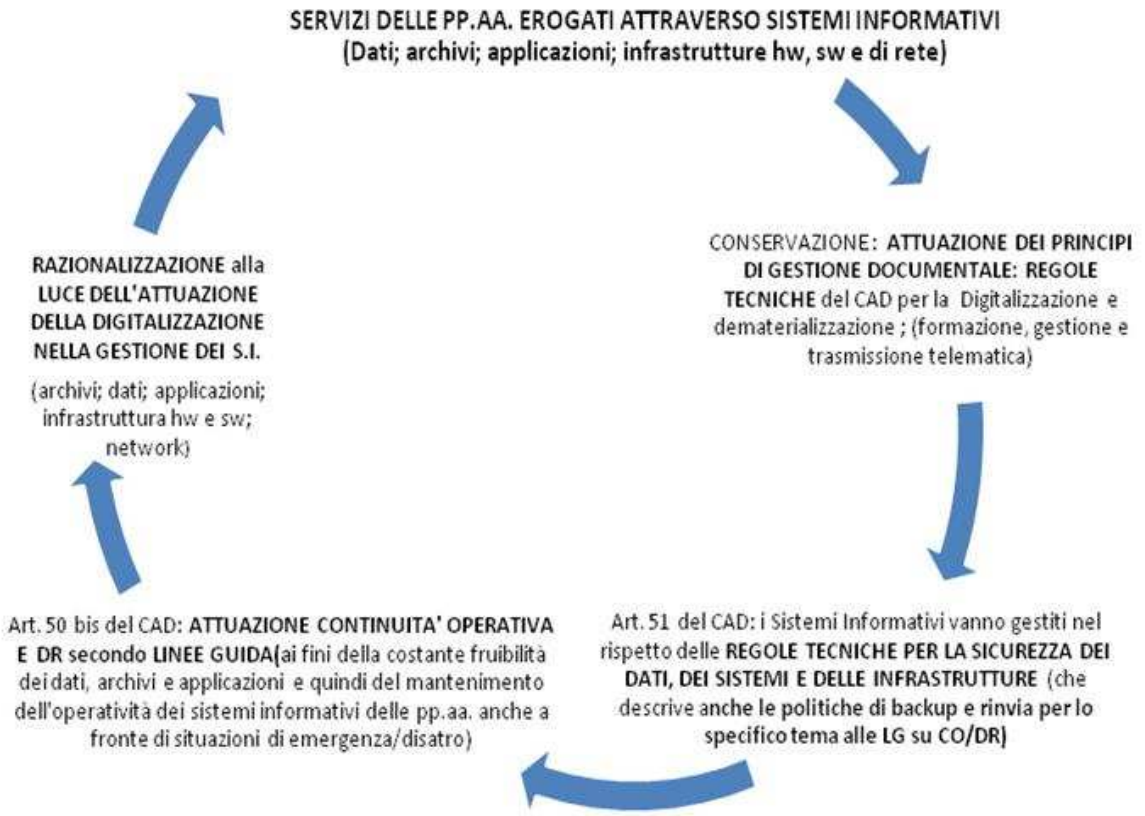
In questo scenario generale la continuità dei sistemi informativi rappresenta per le pubbliche amministrazioni, nell'ambito delle politiche generali per la continuità operativa dell'ente, un aspetto necessario all'erogazione dei servizi a cittadini e imprese e diviene uno strumento utile per assicurare 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.a. predispongono 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 conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

Tale aspetto diviene inderogabile 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:



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 Provincie autonome un ruolo di guida e coordinamento dell'azione di digitalizzazione dell'azione amministrativa svolta a livello locale; a tal fine, le Regioni, le Provincie 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.2*bis* e 3*bis*).

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 affida:

- **a DigitaPA 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 Provincie 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 Analisys (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 prolungate 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.

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.

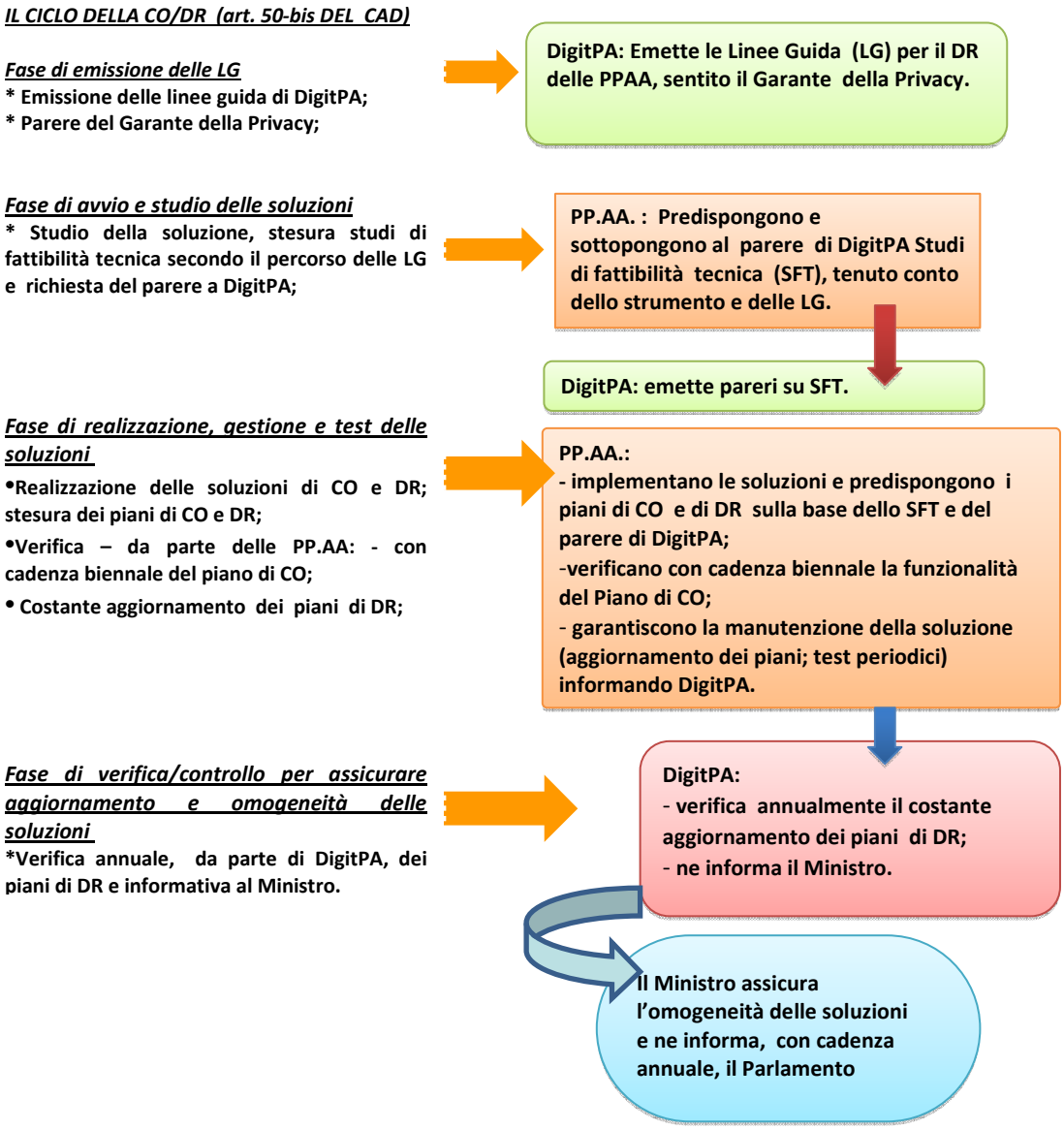
Inoltre, per consentire a DigitPA di verificare annualmente il costante aggiornamento dei piani di Disaster recovery delle Amministrazioni e informare il Ministro per la pubblica amministrazione e l'innovazione, le Amministrazioni dovranno inviare a DigitPA i piani di Disaster Recovery, e devono verificare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



2.5 Collegamento degli adempimenti ex art. 50 bis con le Regole Tecniche previste dall'art. 51 del C.A.D. (Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni)

A completare il quadro giuridico ed operativo descritto è necessario ricordare l'articolo 51, inerente alla "Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni".
Il citato articolo, che prevede che con apposite regole tecniche saranno individuate le modalità per garantire l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture nonché per assicurare che i documenti informatici siano custoditi e controllati in modo tale da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alla finalità della raccolta, affida a DigitPA, il compito di:
a)raccordare le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b)promuovere intese con le analoghe strutture internazionali;

c)segnalare al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle citate regole tecniche parte delle pubbliche amministrazioni.

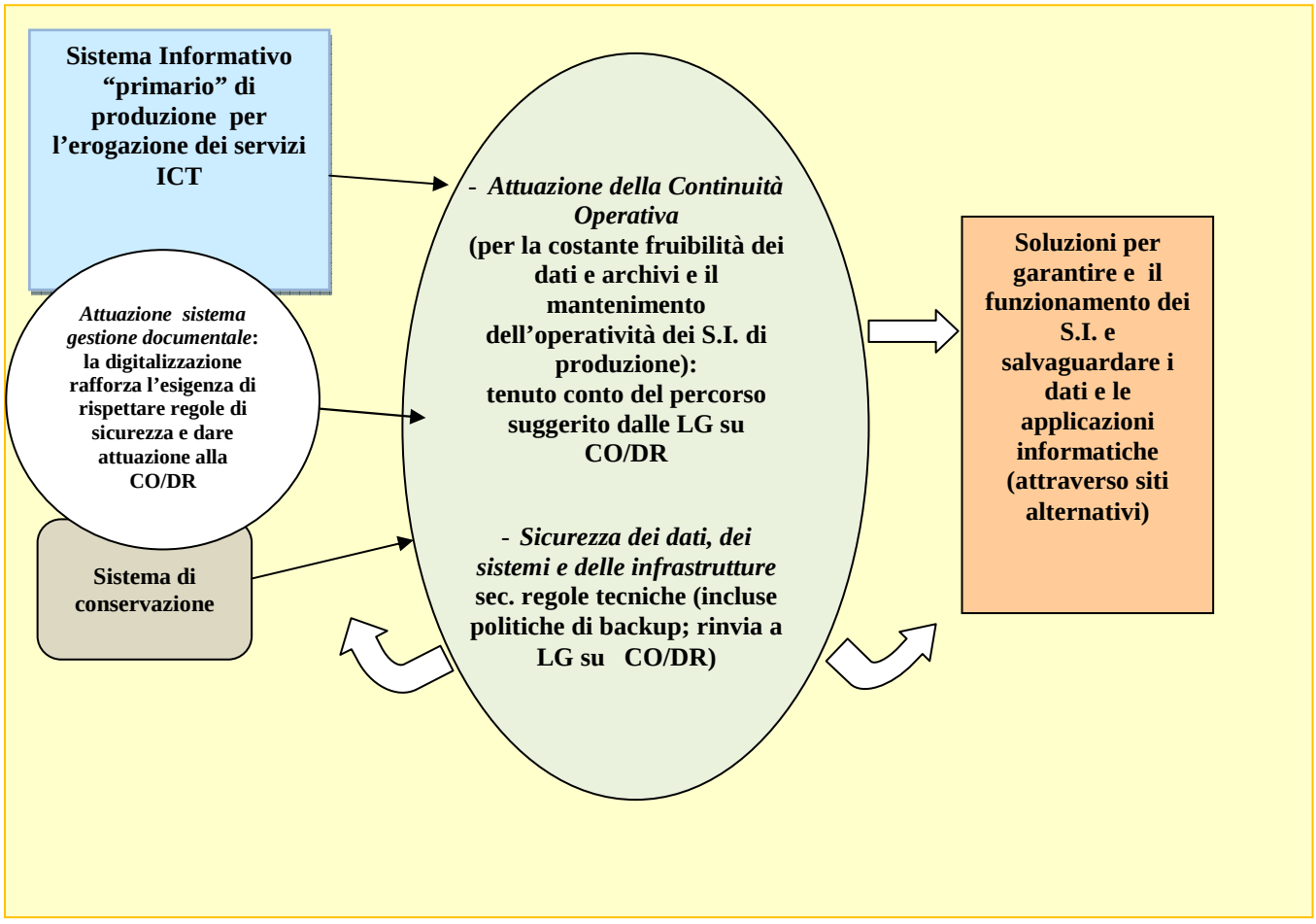
Il secondo comma del richiamato articolo 51 conferma altresì, come si è avuto modo di anticipare, che" *I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta*".

2.6 Collegamento degli adempimenti ex art. 50 bis rispetto alle disposizioni del CAD e alle Regole Tecniche inerenti la formazione, tenuta, conservazione del documento informatico nonché la gestione del documento informatico e dei flussi documentali

Non si può non evidenziare la rilevanza strategica che assume l'adozione di soluzioni di Continuità operativa e Disaster Recovery, considerando che il Codice dell'Amministrazione Digitale impone alle Amministrazioni, fra gli altri, di attivarsi, nel rispetto delle regole tecniche che saranno emanate per la gestione informatica dei documenti, ai sensi delle disposizioni contenute nel C.A.D per garantire la dematerializzazione e digitalizzazione delle modalità di formazione, tenuta, conservazione e gestione del documento informatico e dei flussi documentali.
Ciò rende assolutamente necessaria da parte delle Amministrazioni:

- l'adozione di accurate politiche di backup e di salvataggio degli archivi e dei dati (e quindi sia dei dati strutturati presenti nei data base che dei dati, quali i documenti informatici trattati nell'ambito dei sistemi di gestione documentale, che dei log relativi, che consentono di tracciare le operazioni eseguite);
- l'adozione di soluzioni tecniche per la salvaguardia dei dati e delle applicazioni ed il ripristino a fronte di situazioni di emergenza, come richiesto dall'art. 50 bis cui si riferiscono le presenti linee guida.

Nella figura successiva sono schematizzate le relazioni logiche tra gli adempimenti previsti dal CAD, ai fini della digitalizzazione e sicurezza del servizi ICT, sia per l'attuazione del sistema di gestione documentale sia per la realizzazione di soluzioni di continuità operativa, nel rispetto delle regole tecniche per la gestione documentale e per la sicurezza dei dati, dei sistemi e delle infrastrutture (cui si rinvia).


Sistema Informativo "primario" di produzione per l'erogazione dei servizi ICT
Attuazione sistema gestione documentale: la digitalizzazione rafforza l'esigenza di rispettare regole di sicurezza e dare attuazione alla CO/DR
Sistema di conservazione
- Attuazione della Continuità Operativa (per la costante fruibilità dei dati e archivi e il mantenimento dell'operatività dei S.I. di produzione): tenuto conto del percorso suggerito dalle LG su CO/DR
- Sicurezza dei dati, dei sistemi e delle infrastrutture sec. regole tecniche (incluse politiche di backup; rinvia a LG su CO/DR)
Soluzioni per garantire e il funzionamento dei S.I. e salvaguardare i dati e le applicazioni informatiche (attraverso siti alternativi)

3 STANDARD DI RIFERIMENTO PER L'ATTUAZIONE DELLA CONTINUITÀ OPERATIVA

Il tema degli standard ha un duplice significato nel contesto della Pubblica Amministrazione:

- valutare l'adeguatezza delle forniture o dei servizi richiesti a parametri che garantiscano la rispondenza a tutti i requisiti necessari alle finalità delle forniture o dei servizi;
- permettere l'impiego di certificazioni opportune che garantiscano la qualità del fornitore o del prestatore di servizi.

Nel primo caso è importante avere una conoscenza del panorama di standard attinenti al campo specifico. Nel secondo caso è importante decidere se la richiesta di una certificazione, oltre che essere coerente con le finalità di quanto ricercato, non contrasti con l'apertura necessaria al mercato.

Nel caso della continuità operativa (e del Disaster Recovery visto come componente di questa) esistono molte indicazioni e qualche norma specifica.

Peraltro, benché i contenuti di queste Linee Guida siano rivolti al Disaster Recovery, cioè alla componente ICT della continuità operativa, molto spesso da parte del mercato sono presentati alcuni standard, relativi a quest'ultima, come contestualizzati al Disaster Recovery (anche se referenziato come "business continuity"). In effetti, gli standard in ambito continuità operativa possono benissimo essere utilizzati per un processo di Disaster Recovery. Inoltre, è solo nel campo della "business continuity" che è possibile definire un percorso di certificazione. Infatti, anche se esistono alcuni (pochi) standard specificatamente pensati per il Disaster Recovery, ad oggi manca tra questi uno standard che permetta un percorso di certificazione.

Per queste ragioni, nel seguito è riportata una panoramica che abbraccia tutte queste tipologie di standard.

Nessuno standard internazionale si è ancora imposto nel campo della continuità operativa (CO) in modo indiscutibile e questo vale ancora di più per il Disaster Recovery. Tuttavia alcuni approcci presentano spunti significativi. Peraltro, alcuni standard che trattano altri temi connessi (la sicurezza o il rischio, per esempio), riservano un capitolo o un paragrafo alla CO.

Nel seguito i campi di competenza della continuità operativa e del Disaster Recovery saranno evidenziati ove questo sia significativo.

3.1 Standard internazionali

Gli standard per la continuità operativa sono essenzialmente di origine americana o inglese.
Questi standard consistono generalmente nel descrivere le "best practice" (le "pratiche migliori" o "le buone pratiche") sulla base di esperienze di professionisti della materia.

3.2 Standard di tipo "buone pratiche"

Il termine "standard" può in sé prestarsi a confusione. Non si tratta infatti in questo caso di standard di tipo industriale che danno esattamente le indicazioni da seguire, ma piuttosto di linee guida.

Il tipo di vocabolario e di tono utilizzati in questi testi sono adatti a queste finalità: abbondano le frasi che cominciano con “è opportuno che…” e qualche volta sono fornite varie opzioni tra le quali scegliere.

Questi standard sono un insieme di raccomandazioni basate sulla pratica di un’associazione di professionisti.

Queste associazioni, che pure partecipano a vario titolo ai lavori di normalizzazione nei rispettivi paesi e presso l’ISO, si danno in genere tre obiettivi:

1. condividere e accumulare esperienze per descrivere in modo documentato ciò che risulta la migliore pratica;
2. formare dei professionisti su queste buone pratiche ed emettere certificati di attestazione professionale collegati a vari livelli di esperienza;
3. promuovere questi professionisti certificati stimolando così la sensibilità del mercato sul tema della continuità operativa.

Tra le associazioni che si occupano di continuità operativa, se ne distinguono due:

- Il **DRII** (Disaster Recovery Institute International), che può essere considerato il pioniere di questi argomenti, americano e attivo dal 1988;
- Il **BCI** (Business Continuity Institute), creato nel 1994, inglese, che è un importante riferimento insieme all’organismo di normalizzazione inglese, il BSI (British Standard Intitute) e all’interno dell’organismo di normalizzazione internazionale, l’ISO.

3.3 La base di conoscenza del DRII

Nel 1977 il DRII ha pubblicato una base di conoscenza costituita da dati raccolti al proprio interno sulla continuità operativa. La finalità di questa iniziativa è di presentare in dieci punti gli aspetti che ogni responsabile della continuità operativa deve saper gestire:

1. lo sviluppo e la gestione di un progetto di CO;
2. la valutazione e la gestione del rischio;
3. l’analisi di impatto sulle attività;
4. lo sviluppo di una strategia di continuità;
5. i provvedimenti da mettere in opera immediatamente;
6. la predisposizione di un piano di continuità;
7. i programmi di sensibilizzazione e formazione;
8. la manutenzione e il test del piano di CO;
9. le modalità di comunicazione in caso di crisi;
10. il coordinamento con le autorità.

Questo quadro di riferimento è riconosciuto internazionalmente.

3.4 Lo standard BS 25999

Il BSI, che è, come detto, l’organismo di normalizzazione inglese (equivalente all’UNI in Italia), ha emesso uno standard sul tema della CO: il **BS 25999**. Ad oggi è questo lo standard più avanzato e seguito ed è quindi importante prestarvi attenzione, per varie ragioni:

- concentra un insieme di lavori ed esperienze pratiche molto vasto e significativo;

- la sua diffusione va ben oltre l'Inghilterra: la sua influenza si fa sentire in una cinquantina di paesi.
- l'ISO sta riprendendo molti standard del BSI per renderli standard internazionali, quasi senza alcuna modifica.

3.4.1 BS 25999-1 e BS 25999-2

Come in altri casi di standard (a esempio, quelli sulla sicurezza di processo), lo standard BS 25999 è suddiviso in due parti:

- il BS 25999-1 ("BS 25999-1:2006 Business Continuity Management. Code of Practice"), emesso nel 2006, rappresenta le buone pratiche per la CO;
- il BS 25999-2 ("BS 25999-2:2007 Specification for Business Continuity Management"), emesso nel 2007, descrive la messa in opera del sistema di gestione e del relativo impianto di verifica. Pertanto, rappresenta il riferimento per il percorso della certificazione. Alla data, circa 40 organizzazioni sono certificate BS 25999.

3.4.2 I sei punti del BS 25999-1

Lo standard evidenzia principalmente sei punti:

1. **comprendere l'organizzazione**: si tratta di identificare esattamente i rischi ai quali l'organizzazione è esposta e le attività critiche;
2. **definire le opzioni per la CO**: significa scegliere le possibili opzioni in caso di emergenza e di elencare tutti gli elementi (le infrastrutture, il personale, i siti, ecc.);
3. **sviluppare e attuare la soluzione di CO**: significa produrre il piano di CO, a cominciare dai ruoli e le responsabilità in caso di emergenza e darne attuazione;
4. **introdurre la cultura della CO nell'organizzazione**: sono gli aspetti di sensibilizzazione e formazione, come in altri contesti spesso sottovalutati o trascurati;
5. **verificare la soluzione di CO**: una periodicità di verifica superiore a uno-due anni può rendere gravemente inadeguata la soluzione;
6. **gestire la CO**: sostanzialmente, sovraintendere a tutte le precedenti attività.

3.5 Lo standard BS 25777

Benché lo standard BS 25999 sia spesso riferito allo specifico contesto ICT, quindi agli aspetti più propriamente tecnologici della continuità operativa di pertinenza in genere riferita al Disaster Recovery, si tratta di uno standard rivolto alla continuità complessiva dell'organizzazione. Nel 2008 il BSI ha emesso uno standard (del tipo "buone pratiche") specificatamente dedicato alle componenti ICT dell'organizzazione: il **BS 25777** ("Information and communications technology continuity management - Code of practice"). Si tratta comunque di uno standard che ripercorre quanto previsto nella BS 25999-1 contestualizzandolo all'ICT.
Con l'uscita nel marzo 2011 dello standard ISO 27031 (si veda oltre) questo standard è, in pratica, riassorbito da quello internazionale che, peraltro, deriva in grande parte proprio dal BS 25777.

3.6 I lavori dell'ISO

L'ISO ha preso a considerare un tema a sé stante quello della CO solo da pochi anni, dopo averlo considerato un aspetto comune ad altri contesti. Lo standard più importante, ma in via di definizione