AGENZIA PER L'ITALIA DIGITALE
GESTIONE EX DIGITPA

LINEE GUIDA PER IL DISASTER RECOVERY DELLE PUBBLICHE AMMINISTRAZIONI

ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale

Aggiornamento 2013

GUIDA ALLA LETTURA 5
PERCORSO MINIMO DI LETTURA 6
GLOSSARIO DELLE PRINCIPALI DEFINIZIONI 7
1 OBIETTIVI E SCENARI DELLA CONTINUITÀ OPERATIVA DELLE PUBBLICHE AMMINISTRAZIONI NEL QUADRO NORMATIVO VIGENTE 13
1.1 Il Codice dell'Amministrazione Digitale e il perimetro della Continuità Operativa 13
1.2 La Continuità Operativa e il Disaster Recovery: qualità e continuità di funzionamento dei servizi istituzionali 15
1.3 Il percorso dell'art. 50bis e le Linee Guida: strumenti a supporto per l'individuazione delle soluzioni di Disaster Recovery 16
2 IL CODICE DELL'AMMINISTRAZIONE DIGITALE E LA DIGITAL AGENDA: RUOLI E RESPONSABILITÀ 20
2.1 Obblighi e adempimenti previsti nel Codice in materia di protezione dei dati personali 20
2.2 La centralità della digitalizzazione dell'azione amministrativa e della Continuità operativa 20
2.3 Rapporti tra Stato, Regioni, Province autonome ed enti locali 24
2.4 Ruoli e responsabilità per la realizzazione dei Piani di CO e dei Piani di DR 25
2.5 Continuità operativa, Sicurezza dei dati, dei sistemi e delle infrastrutture nel CAD, Sicurezza delle reti e razionalizzazione dei siti e delle infrastrutture digitali 28
2.6 Continuità operativa e dematerializzazione nel CAD 29
2.7 Lo stato di attuazione dell'art. 50bis 30
2.7.1 I servizi tipici di Comuni, Province, Università, ASL e aziende ospedaliere nelle richieste di parere sugli Studi di Fattibilità Tecnica 31
2.7.2 Dati statistici ricavati dai pareri (Tier, valori di RTO/RPO attesi) 34
2.7.3 Le principali criticità e raccomandazioni nei pareri resi dall'Agenzia 35
3 INFRASTRUTTURE E ORGANIZZAZIONE IT PER LA CONTINUITÀ OPERATIVA 37
3.1 Infrastrutture e sistemi: Cenni ai data center della PA 37
3.1.1. Definizione di Data Center 37
3.1.2 Localizzazione 38
3.1.3 Spazi dedicati al DC 39
3.2 Caratteristiche strutturali del DC 39
3.2.1.Pavimenti e solai 39
3.2.2. Sistemi di illuminazione 39
3.2.3 Cablaggi e telecomunicazioni 39
3.2.4 Armadi rack e cage 40
3.2.5 Sistemi di raffreddamento e climatizzazione 40
3.2.6 Sistemi di alimentazione e di continuità elettrica 41
3.2.6.1 Sistema di distribuzione dell'energia 41
3.2.6.2 Distribuzione dell'energia: rete di terra/UPS/gruppi elettrogeni 41
3.2.6.3 Efficienza energetica 41
3.2.7 Sistemi antincendio e antiallagamento 41
3.2.8 Protezione del Data Center 42

3.2.9 Controllo delle infrastrutture 42
3.3 I processi gestionali 43
3.3.3 Gestione operativa, controllo delle prestazioni e manutenzione programmata 43
3.3.4 Gestione della configurazione, delle capacità e dei processi di approvvigionamento 43
3.3.5 Processi di approvvigionamento 44
3.4 LDS del Data Center 44
3.4.3 Gestione impiantistica industriale – parte elettrica 44
3.4.4 Gestione impiantistica industriale – parte meccanica 45
3.4.5 Gestione Sicurezza Fisica 45
3.4.6 Certificazioni 45
3.5 Strutture per la gestione dell'emergenza: coinvolgimento e ruolo dei vertici dell'amministrazione 45
3.5.3 Descrizione caratteristiche e compiti responsabile CO 45
3.5.4 Strutture per la gestione dell'emergenza: il comitato di crisi 46
4 LA REALIZZAZIONE DELLA CONTINUITÀ OPERATIVA E DELLE SOLUZIONI DI DISASTER RECOVERY 49
4.1 Determinazione delle esigenze di continuità e delle soluzioni 49
4.3 Strumenti per l'autovalutazione 51
4.2.1 Le direttrici di analisi 52
4.2.2 I criteri di stima 52
4.2.3 Le tipologie di soluzioni tecniche 53
4.4 Ulteriori elementi che possono essere tenuti presenti 57
4.3.1 Cenni sulle modalità di realizzazione delle soluzioni 57
4.3.2 Cenni su aspetti tecnologici che possono orientare la scelta delle soluzioni 57
4.3.2.1 La virtualizzazione 57
4.3.2.2 Le soluzioni cloud 58
4.3.2.3 La connettività e gli aspetti di sicurezza della rete 61
5 LO STUDIO DI FATTIBILITÀ E I PIANI DI CO E DI DR DELLE PA 62
5.1 Premessa 62
5.2 Lo Studio di Fattibilità Tecnica: modello di riferimento 63
6 STRUMENTI GIURIDICI E OPERATIVI PER LA ACQUISIZIONE DI UN SERVIZIO DI DR 73
6.1 I possibili servizi minimi essenziali 73
6.2 Possibili percorsi per l'attuazione di soluzioni di CO e di DR 78
6.2.1 Ipotesi A: percorso di attuazione della soluzione di CO e DR interno all'Amministrazione 79
6.2.2 Ipotesi B: percorso di attuazione della soluzione di CO e DR con il supporto parziale di fornitori 79
6.2.3 Ipotesi C: percorso di attuazione della soluzione di CO e DR affidato ai fornitori 80
6.2.4 Outsourcing dei servizi ICT: avvertenze 81
6.2.5 La realizzazione di soluzioni di continuità operativa 81

6.3 Richiami alla principale normativa di riferimento per le procedure di acquisizione di beni e servizi 82
6.4 Le acquisizioni tramite Convenzioni, Accordi Quadro, MEPA e Contratti Quadro 83
6.4.1 Connettività e servizi SPC 84
6.5 Cenni agli strumenti e clausole da adottare per soluzioni cloud che implichino il trasferimento dei dati (rinvio alla normativa comunitaria e ai provvedimenti del Garante per la protezione dei dati personali) 84
7 CONTINUITÀ OPERATIVA E DISASTER RECOVERY DELLE INFRASTRUTTURE CRITICHE 88
7.1 La protezione delle IC in Europa 89
7.2 Cenni alle azioni in Italia 93
7.3 Conclusioni: la sicurezza informatica, la continuità operativa, le infrastrutture critiche 97
8 CONCLUSIONI 99
APPENDICE A: LE POLITICHE DI BACK UP 101
APPENDICE B: GLI STANDARD DI RIFERIMENTO PER L'ATTUAZIONE DELLA CONTINUITÀ OPERATIVA 104
APPENDICE C: MODELLO DI PIANO DI CONTINUITA' ICT 108
APPENDICE D: SPECIFICAZIONI SUGLI STRUMENTI GIURIDICI ED OPERATIVI PER L'ACQUISIZIONE DEI SERVIZI DI CO/DR 117
APPENDICE E: ESEMPI DI LDS 140

GUIDA ALLA LETTURA

Il documento è correlato ai contenuti e redatto ai sensi del c. 3, lettera b) dell'art. 50bis "Continuità operativa" del Codice dell'Amministrazione Digitale.

I contenuti dell'attuale versione delle Linee Guida sono i seguenti:

- il Capitolo 1 definisce, all'interno della più ampia Continuità Operativa Generale dell'Organizzazione, gli obiettivi e gli scenari della Continuità Operativa ICT - nel prosieguo del documento per brevità denominata solo "Continuità Operativa" (CO) – e, in particolare, gli aspetti del Disaster Recovery (DR), previsto nella Continuità Operativa, nell'ambito delle Pubbliche Amministrazioni all'interno del quadro normativo vigente e, anche, alla luce del percorso avviato e condotto a seguito delle Linee Guida, 1° versione, emanate nel novembre 2011;
- il Capitolo 2 descrive il Codice della Amministrazione Digitale, con riferimento specifico alla tematica della Continuità Operativa, illustrando i ruoli e le responsabilità assegnate dallo stesso e dalla Digital Agenda alle Pubbliche Amministrazioni e alla Agenzia per l'Italia Digitale (ex-DigitPA);
- il Capitolo 3 attiene alle infrastrutture ICT e all'organizzazione della Pubblica Amministrazione in materia di Continuità Operativa;
- il Capitolo 4 illustra il percorso per la realizzazione della Continuità Operativa e delle soluzioni di Disaster Recovery nella Pubblica Amministrazione e costituisce una guida sulle modalità con cui affrontare il problema della Continuità Operativa sia dal punto di vista tecnico che dal punto di vista organizzativo. Nel capitolo vengono fornite indicazioni sul percorso e gli strumenti da utilizzare per individuare i Tier (soluzioni tecnologiche) e poi impostare il progetto e definire tempestivamente i Piani di Continuità Operativa e di Disaster Recovery che consentiranno all'Amministrazione di dotarsi di soluzioni di Continuità Operativa al servizio dei compiti istituzionali in linea con il proprio contesto tecnico operativo di riferimento e prevedendo anche gli opportuni meccanismi di verifica periodica e manutenzione nel tempo, indispensabili a rendere la soluzione individuata adeguata anche a fronte di rilevanti variazioni tecnico organizzative;
- il Capitolo 5 illustra lo Studio di Fattibilità Tecnica e fornisce ulteriori suggerimenti, alla luce dei pareri emessi, per la redazione della documentazione da produrre per richiedere il parere ai sensi dell'art. 50bis, c. 4 del CAD;
- il Capitolo 6 fornisce indicazioni in merito alle modalità di approvvigionamento delle forniture e dei servizi necessari alla realizzazione delle soluzione di Disaster Recovery individuate. In detto capitolo, alla luce del lavoro svolto dal Tavolo tecnico a ciò deputato, sono anche individuati i servizi minimi essenziali legati alle soluzioni di Disaster Recovery (schede servizi), esempi di possibile combinazione di dette schede per i vari casi, nonché 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 tratta della Continuità Operativa e delle soluzioni di Disaster Recovery delle Amministrazioni interessate dalla normativa che attiene alla protezione delle infrastrutture critiche, oggetto di recenti interventi normativi a livello europeo e nazionale;
- il Capitolo 8 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 Disaster Recovery ed esempi di livelli di servizio contrattualizzati con i fornitori.

Il documento è stato redatto e curato dal "Gruppo di lavoro per la revisione e aggiornamento delle Linee Guida per il Disaster Recovery delle PPAA", dal Prof Antonio Orlandi (Coordinatore), dalla D.ssa Cristina Di Domenico, dal Dott. Giovanni Rellini Lerz, dall'Ing. Alessandro Alessandroni, dal Dott. Giampaolo La Bruna e dalla D.ssa Diana Bonofiglio.

Hanno partecipato alle attività del Gruppo di lavoro:
CONSIP – Dott.ssa Maria Stella Marotta;
SOGEI: Dott. Massimo Greco; Dott. Henry Zammar;
Banca di Italia – D.ssa Isabella Stefanangeli, Ing. Stefano Simeoni;
Stato Maggiore Difesa – D.ssa Marica Di Camillo; D.ssa Laura Leone;
Arma dei Carabinieri – Maggiore Gianluigi Me;
CONFINDUSTRIA DIGITALE: Giuseppe Neri; Marco Schina (Almaviva); Maurizio Giovanetti (IBM); Francesco Scribano (IBM); Giuseppe Di Natale (HP); Enrico De Simoni (KPMG); D.ssa Paola Colonna (Telecom)
CISIS: Andrea Nicolini

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. 50bis del CAD.

Capitolo 1	OBIETTIVI E SCENARI DELLA CONTINUITÀ OPERATIVA DELLE PUBBLICHE AMMINISTRAZIONI NEL QUADRO NORMATIVO VIGENTE
Capitolo 2	§ 2.2 – La centralità della digitalizzazione dell'azione amministrativa e della Continuità operativa § 2.4 - Ruoli e responsabilità per la realizzazione dei Piani di CO e dei Piani di DR
Capitolo 3	INFRASTRUTTURE E ORGANIZZAZIONE IT PER LA CONTINUITA' OPERATIVA
Capitolo 4	LA REALIZZAZIONE DELLA CONTINUITA' OPERATIVA E DELLE SOLUZIONI DI DR NELLA PA
Capitolo 5	LO STUDIO DI FATTIBILITÀ E I PIANI DI CO E DI DR DELLE PA
Capitolo 6	STRUMENTI GIURIDICI E OPERATIVI PER L'ACQUISIZIONE DI UN SERVIZIO DI DR
Capitolo 7	CONTINUITA' OPERATIVA E DISASTER RECOVERY DELLE INFRASTRUTTURE CRITICHE
APPENDICI	B Gli standard di riferimento per l'attuazione della continuità operativa; C Modello di Piano di Continuità ICT D Specificazioni sugli strumenti giuridici e operativi per l'acquisizione dei servizi di CO/DR

GLOSSARIO DELLE PRINCIPALI DEFINIZIONI

Nell'ambito del presente documento si intende per:

- *Agenzia per l'Italia Digitale (AGID*): istituita con la L. 134/2012 con attribuzione, tra le altre, delle competenze di DigitPA in tema di attuazione dei diritti digitali e di vigilanza sull'attuazione del CAD, con particolare riferimento, in relazione al presente documento, al rispetto delle prescrizioni dell'art. 50bis ("Continuità operativa");

- *Agenda Digitale Europea o Digital Agenda for Europe (DAE):* è una delle iniziative cardine della strategia Europa 2020 (ora Horizon 2020), che grazie a una maggiore diffusione e ad un uso più efficace delle tecnologie digitali nell'ambito della Strategia 2020 (lanciata dalla Commissione europea nel marzo 2010 con l'intento di uscire dalla crisi e di preparare l'economia dell'UE per le sfide del prossimo decennio, raggiungendo alti livelli di occupazione, produttività e coesione sociale e un'economia a basse emissioni di carbonio), ha l'obiettivo di stimolare l'innovazione e la crescita economica e migliorare la vita quotidiana dei cittadini e delle imprese. L'Agenda mira in particolare a: creare i presupposti per un mercato digitale unico e dinamico, che consenta di sfruttare i benefici dell'era digitale; garantire un'effettiva interoperabilità tra i prodotti e i servizi delle tecnologie dell'informazione; adottare una politica rafforzata in materia di sicurezza delle reti e delle informazioni; rendere l'accesso ad internet veloce e superveloce, garantendo la copertura universale della banda larga a velocità sempre maggiori e la promozione di reti di nuova generazione; incentivare la ricerca e l'innovazione in materia di tecnologie digitali, sfruttando il mercato unico; abolire il c.d. Digital Divide, migliorare l'alfabetizzazione, le competenze e l'inclusione nel mondo digitale; ridurre i consumi energetici, migliorare i servizi ai cittadini attraverso l'e-government delle amministrazioni, migliorare l'efficienza dei trasporti e la mobilità, migliorare l'assistenza sanitaria (rafforzare la consapevolezza dei pazienti e favorire l'inclusione dei disabili) ecc. ecc.;

- *Agenda Digitale Italiana (ADI):* è l'insieme degli obiettivi e azioni che l'Italia, attraverso la Cabina di Regia istituita con la legge n. 35/2012 e l'Agenzia per l'Italia Digitale, istituita con la legge n. 134/2012, intende portare avanti per l'attuazione dei *pillar* e azioni della DAE, che comprende, fra le altre, azioni per potenziare la sicurezza dei sistemi e delle infrastrutture;

- *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 e di valutare l'impatto di tale evento sull'operatività dell'Amministrazione, richiamata in appendice al presente documento;

- *Codice dell'Amministrazione Digitale (CAD*): D.Lgs. n. 82/2005 e s.m.i., aggiornato alla luce del D. Lgs. n. 235/2010, dalla L. n. 135 del 7 agosto 2012 e dalla legge n.221/2012 di conversione del D. L. n. 179 del 18 ottobre 2012;

- *Comitato di crisi:* è l'organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività delle risorse coinvolte; è l'organo di direzione strategica dell'intera struttura in occasione dell'apertura dello stato di emergenza ICT e, inoltre, condivide con il responsabile della CO la responsabilità di garanzia e controllo sulla continuità operativa di un Ente o Amministrazione.

- *Continuità Operativa Generale dell'Organizzazione*: condizione in cui, pur in presenza di un'emergenza, sono attive tutte le misure tecnico-organizzative e gestionali volte ad assicurare, al massimo possibile, le prestazioni rese dai processi critici. Le regole per la gestione, a livello generale dell'organizzazione, della continuità operativa dei processi critici in situazioni di emergenza viene definita in un apposito documento (Piano di Continuità Operativa Generale dell'Organizzazione) le cui prescrizioni si applicano alle situazioni di emergenza di rilievo generale;

- *Continuità Operativa ICT (CO):* la capacità di un organizzazione di adottare - per ciascun processo critico e per ciascun servizio istituzionale critico erogato in modalità ICT, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative - misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi e funzioni istituzionali. Il processo ICT è un caso tipico di processo critico;

- *Copia dei dati e delle applicazioni (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 PPAA:* il dato formato o comunque trattato da una PA;

- *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. 50bis del CAD;

- *Disaster:* l'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'organizzazione;

- *Disaster recovery (DR*): nell'ottica dell'art. 50bis 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 Generale dell'Organizzazione*: si può definire tale il Piano che fissa gli obiettivi e i principi da perseguire da parte dell'Organizzazione; descrive i ruoli, le responsabilità, i sistemi di escalation e le procedure per la gestione della Continuità Operativa Generale (e non solo ICT) dell'Amministrazione, tenuto conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche. In realtà particolarmente complesse il Piano può essere solo un documento di primo livello cui vanno associati, per esempio, documenti di secondo livello, quali procedure relative a servizi/processi e/o sistemi specifici (per esempio il Piano di Continuità Operativa ICT) e finanche documenti di terzo livello (per esempio sotto forma di istruzioni di lavoro che riportano indicazioni operative specifiche);

- *Piano di Continuità Operativa ICT (PCO)*: Documento operativo che descrive tutte le attività e modalità finalizzate al ripristino delle funzionalità ICT, a seguito di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi classificati come "critici"; per una realtà di dimensioni limitate, soprattutto sotto il profilo ICT, il Piano di Continuità Operativa ICT e il Piano di DR possono coincidere ma dovrà comunque essere presente la

componente dedicata al Disaster Recovery. In realtà particolarmente complesse, all'opposto, 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 (ad esempio il Piano di Disaster Recovery) 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/DRP):* Documento operativo che descrive tutte le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità delle funzioni ICT a supporto dei servizi definiti "critici", il ripristino delle stesse, entro un arco temporale predefinito, tale da rendere, il più possibile, minime le interruzioni nell'erogazione dei servizi. Si evidenzia che il PDR/DRP è la sezione del PCO che descrive le attività di ripristino del sistema informativo, costituisce parte integrante del PCO e stabilisce le misure tecniche ed organizzative per assicurare l'erogazione dei servizi classificati come critici (e delle procedure e applicazioni informatiche correlate) tramite le risorse hw, sw e di connettività presso un CED alternativo a quello/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 o meno 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;

- *Processo critico*: processo essenziale per l'erogazione dei servizi di natura istituzionale ovvero di quelli a loro diretto supporto e la cui interruzione, per un tempo superiore a un limite predefinito, provoca danni non accettabili dal punto di vista organizzativo sociale, reputazionale, economico-finanziario. Il management dell'organizzazione attribuisce l'attributo "critico" a un processo sulla base dello svolgimento di una BIA su quel processo e/o su considerazioni di carattere più generale legate a fattori sociali, ambientali, territoriali, politici, ecc.;

- *Responsabile della Continuità Operativa*: il responsabile che ha il ruolo di supportare l'Amministrazione per predisporre tutte le misure necessarie per ridurre l'impatto di un'emergenza ICT e, reagire prontamente e in maniera efficace in caso di interruzione dei servizi ICT erogati a causa di un disastro. Inoltre ha la responsabilità' di sviluppare e mantenere aggiornato il piano di Continuità Operativa ICT. Il Responsabile della Continuità Operativa e' membro del Comitato di crisi;

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

- *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 (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto;

- *RTO: Recovery Time Objective,* indica il tempo di ripristino del servizio: è la durata di tempo 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;

- *Servizi istituzionali ICT:* la base di partenza nell'individuazione delle soluzioni di salvaguardia dei dati e delle applicazioni; sono i processi critici e i servizi istituzionali che l'ente eroga in modalità ICT o mediante l'apporto delle tecnologie ICT;

- *Servizi minimi essenziali:* i servizi necessari per dotarsi di soluzioni di Disaster Recovery o anche per migliorare quelle esistenti descritti nelle Schede Servizio richiamate nel presente documento;

- *Situazione di emergenza generale*: situazione nella quale si determinano le condizioni per una riduzione rilevante o per l'interruzione delle prestazioni rese dai processi critici. All'emergenza effettiva è assimilata anche l'emergenza potenziale, nella quale cioè il rischio di riduzione rilevante o di interruzione dell'operatività è elevato e imminente;

- *Soluzione Tecnica per la CO/DR:* rappresenta la soluzione ICT da implementare per il soddisfacimento del Tier scelto per assicurare la CO e che viene identificato tramite lo strumento di autovalutazione;

- *Soluzione Tecnologica per la CO/DR (TIER):* comprende la realizzazione e la gestione di tools, sistemi, tecniche, metodologie tecnico-organizzative, utili a ottenere un determinato livello di servizio per la continuità operativa;

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

- *Strumento di autovalutazione:*è il tool messo a disposizione dall'Agenzia sul proprio sito - ai fini della predisposizione degli studi di fattibilità tecnica e dei PCO e PDR - per supportare le Amministrazioni nell'identificazione delle soluzioni tecnologiche idonee alla CO (Tier da 1 a 6), avendo come base di partenza essenzialmente i "servizi" che l'ente eroga nei confronti della collettività;

- *SPC:* Sistema Pubblico di Connettività (artt. 73 e segg. del CAD); 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 PA, 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 PA.;

- *Tier:* letteralmente, livello, grado. Nel presente documento:
  - nel capitolo 3 (e nell'ambito delle Linee Guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione) il termine tier viene utilizzato nell'accezione dello standard TIA-942 che classifica i Data Center in 4 livelli ("Tier") caratterizzati da caratteristiche progressivamente migliorative, ai fini della affidabilità e disponibilità del Data Center;

- nel capitolo 4 (e nel tool di autovalutazione predisposto dall'Agenzia) il termine tier viene utilizzato nell'accezione di tipologie di soluzioni tecnologiche per la CO/DR, articolate in 6 livelli ("Tier"), utili a ottenere valori progressivamente inferiori di RTO e RPO.

1 OBIETTIVI E SCENARI DELLA CONTINUITÀ OPERATIVA DELLE PUBBLICHE AMMINISTRAZIONI NEL QUADRO NORMATIVO VIGENTE

1.1 Il Codice dell'Amministrazione Digitale e il perimetro della Continuità Operativa

Il CAD sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la digitalizzazione dei servizi (art. 15 "*Digitalizzazione e riorganizzazione*"). Da tale indicazione consegue, per la Pubblica Amministrazione (nel prosieguo PA), anche l'obbligo di assicurare la continuità dei processi che presiedono alla erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese. Questa affermazione assume particolare significato a fronte del sempre maggiore utilizzo delle tecnologie ICT nella gestione dei dati e dei procedimenti dei singoli enti, che rende necessario adottare tutte le iniziative tese a salvaguardare l'integrità, la disponibilità, la continuità nella fruibilità dei dati. 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 per il quale è necessario garantire salvaguardia e disponibilità, anche attraverso l'adozione di misure di sicurezza e di soluzioni atte a garantire la continuità di funzionamento dei sistemi informativi.
La Continuità Operativa Generale dell'Organizzazione/Amministrazione è da sempre stata intesa come l'insieme delle attività e delle politiche adottate per ottemperare all'obbligo di assicurare la continuità nel funzionamento dell'organizzazione.
Questo 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.

Come detto i dati, le informazioni e le applicazioni che li trattano sono ormai parte essenziale ed indispensabile per lo svolgimento delle funzioni istituzionali di un ente/organizzazione ed è necessario quindi garantirne la salvaguardia, la disponibilità, la sicurezza, unitamente a confidenzialità ed integrità: il tema della continuità operativa deve quindi essere parte integrante dei processi e delle politiche di sicurezza di un'organizzazione. In quest'ottica l'attuazione degli obblighi imposti dall'art. 50 bis del CAD conduce le Amministrazioni ad adottare un percorso complessivo in materia di sicurezza di tutta l'organizzazione, coerentemente con il quadro normativo richiamato, e può anche essere un ottima occasione per rivisitare e razionalizzare le risorse dedicate.
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, visto che non si può più contare su un backup basato sulla documentazione cartacea. Anche in questo quadro l'adozione di soluzioni di DR diviene un prerequisito indispensabile per garantire la continuità di svolgimento dei processi digitalizzati.

Da quanto detto consegue che la continuità dei servizi informatici rappresenta un impegno inderogabile per la PA che deve 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.

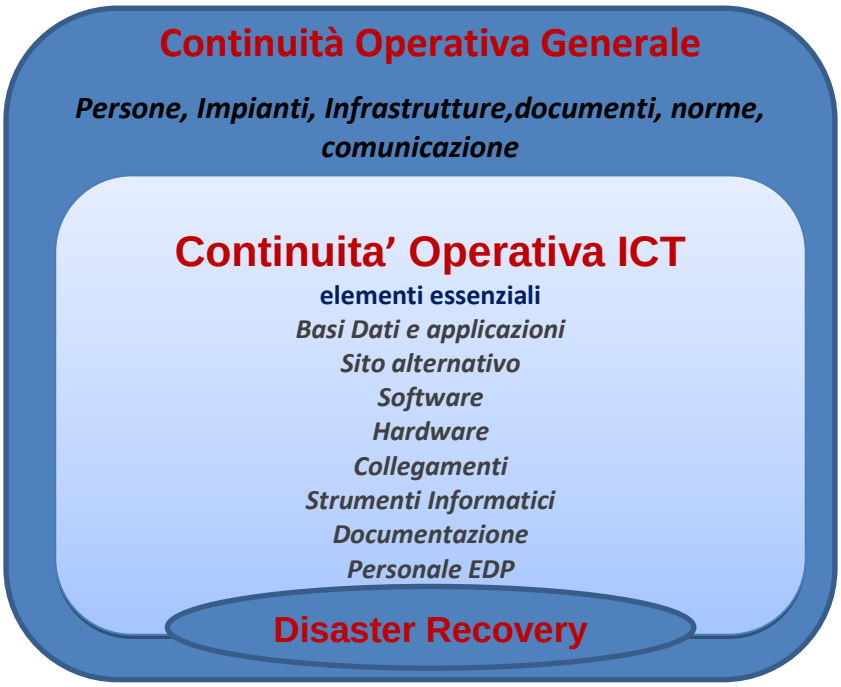
Le espressioni Disaster Recovery, Continuità Operativa ICT e Continuità Operativa Generale dell'Organizzazione sono usate con varie accezioni e, talvolta, erroneamente come sinonimi. Proviamo a fare chiarezza sui termini e su quali siano i reciproci rapporti per meglio definire l'argomento.

La Continuità Operativa Generale riguarda l'intera Organizzazione/Amministrazione e non è oggetto del presente documento; oggetto del documento, invece, sono la Continuità Operativa ICT e il Disaster Recovery.

La Continuità Operativa ICT riguarda il processo critico ICT che, nel caso di grave e prolungata indisponibilità dei sistemi informativi (disservizio incompatibile con le esigenze di continuità di funzionamento dell'Amministrazione), prevede anche il Disaster Recovery per garantire il ripristino dello stato del Sistema Informativo (o di parte di esso), per riportarlo alle condizioni di funzionamento e di operatività antecedenti all'evento disastroso.

Sempre in un'ottica di chiarimento complessivo sul tema della continuità, va segnalato che la Continuità Operativa ICT non deve preoccuparsi solo della disponibilità dei sistemi informativi (scenario risorse informatiche, di cui il Disaster Recovery è la misura estrema di continuità), ma anche della disponibilità delle risorse umane ICT (scenario risorse umane: ad esempio, in una situazione di pandemia o non previsione di risorse alternative), della disponibilità e fruibilità della logistica (scenario risorse logistiche: ad esempio, impossibilità di raggiungere il sito elaborativo o mancanza di riscaldamento/condizionamento degli ambienti del sito), della disponibilità della energia elettrica (scenario energia elettrica: ad esempio, non previsione di fonti alternative di alimentazione). Scenari che potrebbero essere, anche contemporaneamente, coinvolti dall'evento.

La figura seguente, in modo sempre estremamente schematico, prova a illustrare quanto detto e gli elementi essenziali della Continuità Operativa ICT, ivi compreso il DR:



La figura vuole evidenziare che se - a seguito di eventi gravi e imprevisti - si decidesse di attuare le politiche di Disaster Recovery per ripristinare la normale operatività dei processi critici ICT, ma si riuscisse a superare l'emergenza nei tempi pattuiti, contenendo i danni e il disservizio in ambito puramente ICT, non sarebbe necessario adottare anche le misure previste dai piani Continuità Operativa Generale che riguardano altri e fondamentali aspetti dell'operatività aziendale (salvaguardia del personale, impianti, logistica, sicurezza degli edifici, documentazione, ecc.).

Nel seguito del documento la gestione della continuità del servizio sarà associata alle conseguenze di eventi di natura eccezionale che impattano il processo critico ICT e che quindi potrebbero avere conseguenze sui servizi istituzionali dell'Amministrazione, resi alla collettività e agli utenti.

1.2 La Continuità Operativa e il Disaster Recovery: qualità e continuità di funzionamento dei servizi istituzionali

Come detto, la CO deve 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 e concordati.

A tal fine, il perimetro di competenza della CO 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 a supporto dei 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 CAD (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 almeno:

- 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 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. 50bis 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.
La base di partenza nell'individuazione delle soluzioni di salvaguardia dei dati e delle applicazioni sono i processi critici e i servizi istituzionali che l'ente eroga in modalità ICT o mediante l'apporto delle tecnologie ICT.

1.3 Il percorso dell'art. 50bis e le Linee Guida: strumenti a supporto per l'individuazione delle soluzioni di Disaster Recovery

Com'è noto, l'articolo 50bis del CAD delinea gli obblighi, gli adempimenti e i compiti che spettano alle PPAA e all'Agenzia per l'Italia Digitale, ai fini dell'attuazione della CO e delle indispensabili soluzioni di DR, richiedendo che le PPAA definiscano i PCO e i PDR sulla base di appositi e dettagliati studi di fattibilità tecnica" [per i quali] "è obbligatoriamente acquisito il parere" dell'Agenzia.

Per supportare le PPAA nell'attuazione degli adempimenti previsti dal citato articolo a novembre 2011 sono state emanate le "Linee guida per il Disaster Recovery delle PPAA" e la relativa Circolare del 1 dicembre 2011, n. 58, mettendo, inoltre, a disposizione delle Amministrazioni:

- un apposito strumento di autovalutazione come ausilio nella valutazione della criticità dei servizi offerti all'utenza e nell'individuazione delle soluzioni tecniche a supporto della loro continuità;

- raccomandazioni a supporto dell'individuazione dei servizi minimi essenziali per l'adozione delle soluzioni di DR, in linea con l'art. 50bis del CAD;
- indicazioni a supporto delle attività di redazione dei documenti da allegare alla richiesta di parere sugli studi di fattibilità tecnica;
- suggerimenti per la redazione dei piani, per la individuazione delle componenti essenziali all'attuazione di soluzioni di CO e di DR, nonché per la verifica e la manutenzione della soluzione.

Compito dell'Agenzia per l'Italia Digitale è quello di mantenere costantemente aggiornate le Linee Guida pubblicate a novembre 2011 sia alla luce dell'esperienza maturata nell'emissione dei pareri sugli studi di fattibilità tecnica, sia alla luce delle evidenze emerse dalle attività di verifica del costante aggiornamento e manutenzione delle soluzioni di DR sia alla luce delle eventuali evoluzioni 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.

Ad oggi, al fine di coadiuvare le Amministrazioni, è stata realizzata un'applicazione *online* (sul sito istituzionale di AGID) per la valutazione della criticità dei processi che erogano servizi all'utenza.

Sono state definite nel numero e nei contenuti i servizi ritenuti attinenti al tema CO/DR; questo lavoro, essendo stato condiviso con le rappresentanze dei fornitori, costituisce un vero e proprio standard di riferimento nazionale (e verrà diffusamente illustrato nel prosieguo).

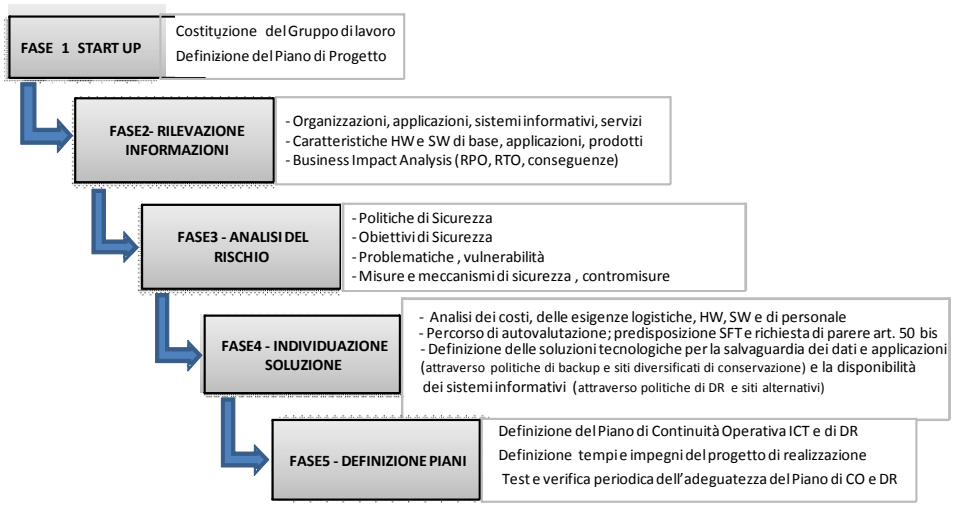
Rispetto al momento di emanazione della prima versione delle Linee Guida, sono stati emessi circa 800 pareri: nel documento si darà evidenza, ove ritenuto utile, sia di quanto emerso nel rapporto con le Amministrazioni che hanno richiesto parere sia dello stato di avanzamento del percorso di attuazione dell'art. 50-bis.

Anche se non solamente legata al DR delle PA, si è ritenuto opportuno avviare un'importante iniziativa nel campo dei data center della PA, costituita da una rilevazione di alcune caratteristiche essenziali di detti data center, fra cui varie relative alla sicurezza IT; questa iniziativa costituirà un fondamentale elemento di partenza per considerazioni sulla razionalizzazione dei DC della PA (come verrà meglio illustrato nel successivo Capitolo 3, cui si rimanda), in linea con quanto disposto del resto dalla legge n. 221/2012.

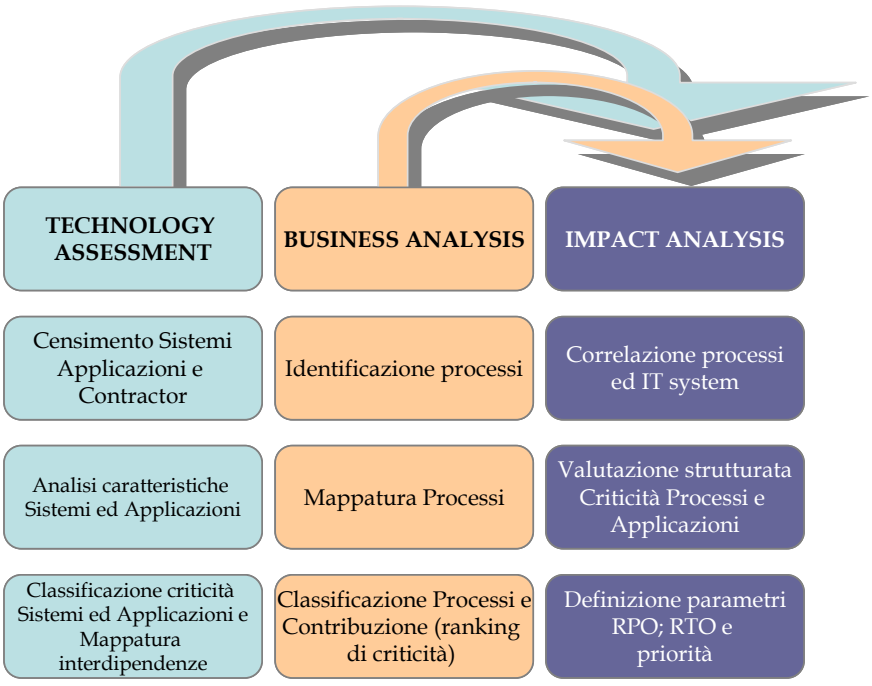
Il raggiungimento di un adeguato livello di CO può essere descritto come un "Processo" articolato che interessa varie componenti tecniche e organizzative, e vari livelli dell'Organizzazione.
Le attività di pianificazione, progettazione e definizione della soluzione (quali momenti del ciclo di attuazione della CO), nel loro insieme, possono essere articolate in una serie di fasi che, sostanzialmente, prevedono:

- la preliminare rilevazione della situazione attuale (in termini di strutture organizzative, processi e procedure, nonché di infrastrutture tecnologiche);
- la successiva analisi degli impatti di situazioni di indisponibilità e l'analisi degli impatti del rischio, per l'individuazione delle aree problematiche e delle contromisure da adottare;
- l'individuazione della soluzione;
- la predisposizione dello studio di fattibilità tecnica e la richiesta e acquisizione del prescritto parere dell'Agenzia per l'Italia Digitale;
- la predisposizione del PCO e del PDR,

come illustrato nello schema seguente:

Ciclo di Vita Metodologico	Output	Strumenti e adempimenti di base
	Rilevazione servizi istituzionali critici	Linee Guida per il DR (presente versione)
	BIA/RA	Metodologia BIA/RA scelta dall'Amm.ne In ogni caso impiego del tool di autovalutazione dell'AGID
	SFT	Modello SFT (Linee Guida per il DR, presente versione) Parere 50bis
	Piano CO e Piano di DR	Standard e Linee Guida per il DR (presente versione)

Il percorso di autovalutazione proposto nel documento è uno strumento che utilizza le informazioni derivate da un assessment tecnologico interno all'organizzazione, dall'analisi dei processi e della loro interrelazione e nonché le informazioni derivanti da un'eventuale analisi del rischio.
Tali azioni possono essere svolte dall'organizzazione in maniera autonoma e con gli strumenti che ritiene più idonei, (come schematicamente illustrato nella figura seguente):



Fasi di assessment, analisi e verifica dei rischi e degli Impatti (Business Impact Analysis), utili al percorso di autovalutazione

Resta fermo che ai fini della redazione dello SFT è necessario utilizzare i risultati del tool di autovalutazione.
La norma prevede anche la verifica annuale del costante aggiornamento dei PDR, con l'obiettivo di assicurare l'omogeneità delle soluzioni di CO e di informare al riguardo, con cadenza annuale, il Parlamento.
A tal fine, come previsto dalla circolare 58/2011, sia le Amministrazioni che avranno chiesto e ricevuto il parere sullo Studio di Fattibilità Tecnica, sia quelle che sono tenute alla verifica annuale prevista dalla norma, devono inviare il PDR all'Agenzia: per le verifiche richieste dalla norma e per garantire il monitoraggio annuale del costante aggiornamento dei PDR delle Amministrazione, la circolare richiamata prevede, infatti, l'invio del PDR con cadenza annuale, unitamente a una dichiarazione che:

- descriva tutte le modifiche apportate al Piano di DR trasmesso e le motivazioni a supporto di tali interventi;

  oppure
- specifichi che nell'anno di riferimento il Piano non è stato modificato in alcuna sua parte.

Obiettivo delle presenti Linee guida è quello di fornire ulteriori suggerimenti e indicazioni per ottemperare agli obblighi derivanti dall'art 50bis del CAD, obblighi che saranno più diffusamente richiamati nel successivo Capitolo 2.
Il documento si propone di essere utilmente adottato dalle Amministrazioni che:

- già si sono dotate dei piani previsti dall'art. 50bis per assicurare soluzioni 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;
- hanno già provveduto a richiedere il parere sullo Studio di Fattibilità Tecnica, ai sensi del c. 4 dell'art. 50bis;
- devono ancora dotarsi dei piani previsti dall'art. 50bis per assicurare soluzioni di CO e di DR e avviare il percorso del citato c. 4 dell'art. 50bis del CAD e possono trovare un valido orientamento per ottemperare agli obblighi imposti dall'art. 50bis del CAD.

Tenuto conto del percorso avviato e in corso per l'attuazione dell'art. 50bis, nella presente versione delle Linee Guida si darà evidenza, nei vari capitoli e paragrafi di quanto emerso nei pareri emessi e nelle attività svolte prima da DigitPA e poi dall'Agenzia nel periodo di vigenza delle Linee Guida di novembre 2011.

2 IL CODICE DELL'AMMINISTRAZIONE DIGITALE E LA DIGITAL AGENDA: RUOLI E RESPONSABILITÀ

2.1 Obblighi e adempimenti previsti nel Codice in materia di protezione dei dati personali

Il D. Lgs. 196/2003 e s.m.i. contenente le disposizioni del "Codice in materia di Protezione dei dati personali", prevede importanti adempimenti in capo alle PPAA 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 dei dati e delle informazioni.
L'art. 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'art. 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. *…*
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.*

2.2 La centralità della digitalizzazione dell'azione amministrativa e della Continuità operativa

Come si è avuto modo di evidenziare nelle Linee guida pubblicate a novembre 2011, l'importanza delle politiche che vengono adottate per garantire la continuità di funzionamento dei sistemi informativi di cui le Amministrazioni si avvalgono per lo svolgimento delle proprie funzioni istituzionali, è confermata nel quadro normativo vigente:

- dall'art. 97 della Costituzione che sancendo che gli uffici pubblici devono essere organizzati in modo che siano garantiti il buon funzionamento e l'imparzialità dell'Amministrazione, impone anche l'obbligo di assicurare la continuità dei procedimenti e servizi resi dalle PPAA, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese;
- dal Codice in materia di Protezione dei dati personali e s.m.i., dalla normativa sui collaudi, dal T.U. sulla sicurezza nel lavoro – D. Lgs. 81/2008 e s.m.i. al DPCM 01.04.2008, ecc. che impongono alle Amministrazioni l'adozione di misure e politiche di sicurezza;

- dall'art. 50bis del CAD che ha reso l'adozione di soluzioni di CO e DR un obbligo cui ottemperare, predisponendo i PCO e PDR previo parere sullo Studio di Fattibilità tecnica;
- dall'art. 51 del CAD (inerente la "Sicurezza dei dati, dei sistemi e delle infrastrutture"), e dalle relative regole tecniche che verranno a tal fine emanate;
- dalla legge 3 agosto 2007, n. 124, così come innovata dalla legge n. 133 del 2012, attinente più in generale ai sistemi per garantire la sicurezza della Repubblica, e s.m.i;
- dal quadro giuridico attinente alle infrastrutture critiche, più dettagliatamente illustrato nel successivo capitolo 7;
- da quanto indicato nel DPCM del 24 gennaio 2013 recante indirizzi per la protezione cybernetica e la sicurezza informatica nazionale, diretto ad accrescere le capacità del Paese di confrontarsi con le minacce alla sicurezza informatica e che pone le basi per un sistema organico, all'interno del quale, sotto la guida del Presidente del Consiglio, le varie istanze competenti potranno esercitare in sinergia le rispettive competenze.

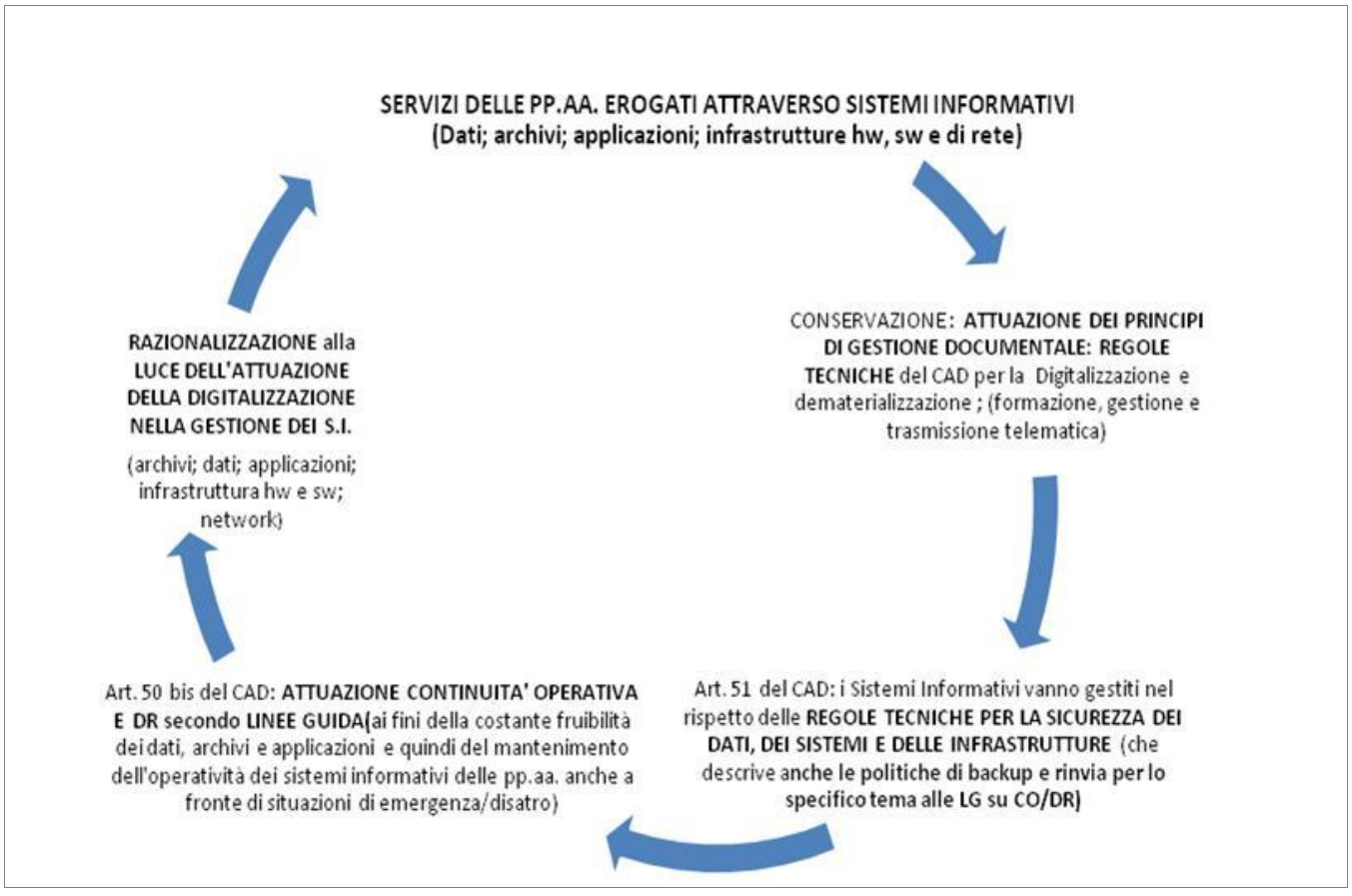
Il CAD ha rafforzato ulteriormente il quadro giuridico descritto e l'obbligo delle PPAA di assicurare oltreché la corretta formazione, raccolta e conservazione dei dati, la costante operatività dei sistemi informativi quale presupposto fondamentale per la qualità e costante fruibilità dei dati stessi, delle informazioni e dei servizi che le stesse PPAA rendono ai cittadini e alle imprese ad es. per le comunicazioni in via telematica, per lo scambio delle certificazioni sanitarie, per lo svolgimento dei pagamenti elettronici ecc..

L'art. 2 del CAD aggiornato (che attiene alle "Finalità e all'ambito di applicazione") precisa che:
"*1. 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 PPAA di cui all'articolo 1, c. 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 PA, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, c. 5, della L. 30 dicembre 2004, n. 311.".

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 art. 2 prevede che: *"Le PPAA 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, nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per la garanzia dei diritti dei cittadini e delle imprese".*
Ulteriori aspetti e disposizioni che compongono il quadro normativo vigente, più direttamente connessi alle procedure di acquisizione e realizzazione delle soluzioni di DR, sono trattati e richiamati nel successivo Capitolo 6, inerente agli "Strumenti giuridici e operativi per l'acquisizione di un servizio di DR" e in appendice al presente documento.

La crescente complessità delle attività legate alla PA, 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 ottica è quindi necessario che, in tema di sicurezza, le PPAA adottino strategie e misure tecnico-operative tali da garantire la continuità di funzionamento dei sistemi informativi attraverso i quali esse assicurano lo svolgimento dei rispettivi compiti istituzionali e l'erogazione dei servizi all'utenza.
Per assicurare la CO, le PPAA devono prevedere, nella gestione ordinaria dei propri servizi ICT, metodologie, strumenti e procedure per fronteggiare ogni possibile evento che metta a rischio la disponibilità del proprio Sistema Informativo (fermi prolungati o reiterate interruzioni), al fine di evitare, o almeno minimizzare, gli impatti negativi e disservizi nei procedimenti svolti e nei servizi erogati all'utenza.
L'attuazione della CO risulta quindi un adempimento inderogabile, tenuto anche conto delle disposizioni in tema di sicurezza, dematerializzazione e conservazione, fra i quali, in particolare, gli articoli 42, 43, 44 del CAD (inerenti rispettivamente la "*Dematerializzazione dei documenti delle Pubbliche Amministrazioni", la "Riproduzione e conservazione dei documenti", il sistema di conservazione dei documenti informatici e i requisiti relativi*) 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 tema di digitalizzazione, gestione documentale, attuazione della continuità operativa ICT, garanzia della sicurezza dei *dati, sistemi e infrastrutture*

Il quadro normativo vigente rafforza ulteriormente l'importanza della CO. La Digital Agenda già prevede fra le varie azioni e pillar, definiti dallo Stato, l'abolizione del Digital Divide, la promozione delle reti di nuova generazione, la creazione della infrastrutture di sicurezza, nonché delle strutture di base per l'utilizzo estensivo delle tecnologie ICT sia per le attività della collettività, fra cui ad es. per

le attività di e-commerce e per le fasi di pagamento, sia nell'attuazione dei procedimenti delle Amministrazioni che si avvalgono dell'ICT.

Per rendere concrete e operative le azioni della Digital Agenda, l'Agenzia per l'Italia Digitale, che è succeduta nelle attività e nelle funzioni istituzionali di DigitPA ([1]) ha fra l'altro il compito di:

- svolgere le funzioni di coordinamento, di indirizzo e regolazione affidate a DigitPA dalla normativa vigente e, in particolare, dall'articolo 3 del D. Lgs. 177/2009;
- svolgere le funzioni affidate all'ISCOM in materia di sicurezza delle reti;
- assicurare il coordinamento informatico dell'Amministrazione statale, regionale e locale, in attuazione dell'art. 117, secondo c., lettera r), della Costituzione;
- assicurare l'uniformità tecnica dei sistemi informativi pubblici destinati ad erogare servizi ai cittadini ed alle imprese, garantendo livelli omogenei di qualità e fruibilità sul territorio nazionale, nonché la piena integrazione a livello europeo;
- supportare e diffondere le iniziative in materia di digitalizzazione dei flussi documentali delle Amministrazioni, ai fini della piena ed effettiva attuazione del diritto all'uso delle tecnologie di cui all'articolo 3 del Codice dell'Amministrazione digitale.

Più in particolare, nell'art. 20 della citata L. 134/2012 e s.m.i., viene specificato che l'Agenzia per l'Italia Digitale esercita le sue funzioni nei confronti delle pubbliche amministrazioni allo scopo di promuovere la diffusione delle tecnologie digitali nel Paese e di razionalizzare la spesa pubblica. A tal fine l'Agenzia:
…." detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità dei linguaggi, delle procedure e degli standard, anche di tipo aperto, anche sulla base degli studi e delle analisi effettuate a tal scopo dall'Istituto Superiore delle Comunicazioni del Ministero dello sviluppo economico, in modo da assicurare anche la piena interoperabilità e cooperazione applicativa tra i sistemi informatici della pubblica amministrazione e tra questi e i sistemi dell'Unione europea;
.." assicura l'omogeneità, mediante il necessario coordinamento tecnico, dei sistemi informativi pubblici destinati ad erogare servizi ai cittadini ed alle imprese, garantendo livelli uniformi di qualità e fruibilità sul territorio nazionale, nonché la piena integrazione a livello europeo….."

Pertanto, l'Agenzia, in ossequio a quanto disposto dal quadro normativo richiamato, è tenuta a dettare raccomandazioni, strategie, norme tecniche e intende curare la sensibilizzazione e alfabetizzazione del personale in materia di sicurezza informatica e di relative emergenze, curando fra gli altri:

- la diffusione di metodologie di rilevazione ed analisi dei rischi connessi all'impiego di tecnologie evolute, nel quadro della riservatezza e della sicurezza;
- l'avvio di iniziative di automazione;
- metodologie di esame, stima e adozione delle misure di protezione necessarie.

[1] il D.L. n. 83/2012, così come convertito nella L. n. 134/2012, ha istituito l'Agenzia per l'Italia Digitale, che è preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana, in coerenza con gli indirizzi elaborati dalla Cabina di regia di cui all'articolo 47 del D. L. 9 febbraio 2012, n. 5, convertito in L. con modificazioni dalla L. 4 aprile 2012, n. 35, e con l'Agenda digitale europea.

L'Agenzia, attraverso l'Ufficio Sicurezza Informatica e Continuità Operativa d'intesa e con la partecipazione anche finanziaria delle Amministrazioni interessate, può provvedere inoltre a:

- promuovere progetti coerenti con gli obiettivi di cui sopra;
- accertare periodicamente, il livello di sicurezza e riservatezza dei sistemi informatici e delle reti telematiche geografiche e locali utilizzate dalle Amministrazioni stesse;
- proporre interventi correttivi e suggerire rimedi alle eventuali carenze tecniche, procedurali e organizzative rilevate in sede di riscontro periodico,

al fine di diffondere la cultura della continuità di servizio e della sicurezza informatica e incrementare la reattività delle Amministrazioni a fronte di emergenze e/o potenziali minacce.

Anche le direttive di azione tratteggiate del c.d. Decreto digitalia (denominato anche "crescitalia. 2.0"), ovvero dal D. L. n. 179 del 18 ottobre 2012, così come convertito nella legge n. 221 del 2012 contenente "ulteriori misure urgenti per la crescita del Paese" e che continuano a porre l'attenzione, quali fattori essenziali di progresso e innovazione, allo sviluppo dell'economia digitale, all'alfabetizzazione informatica, alla realizzazione dell'anagrafe nazionale della popolazione residente, all'attuazione degli *open data* della PA, al potenziamento delle trasmissioni per via telematica di certificazioni, istanze, comunicazioni, all'attuazione della c.d. "scuola digitale", dei pagamenti in modalità informatica, della c.d. giustizia digitale, nonché alla realizzazione delle c.d. comunità intelligenti ecc.., confermano l'importanza dell'adozione di misure di sicurezza e continuità operativa nei procedimenti e servizi istituzionali delle PPAA.

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 all'Agenzia per l'Italia Digitale, meritano particolare attenzione le novità introdotte in materia di rapporti tra Stato ed enti locali.

Il testo aggiornato dell'art. 14 del CAD, che attiene ai "Rapporti tra Stato, Regioni e autonomie locali" stabilisce:

1. *In attuazione del disposto dell'art. 117, secondo comma, lettera r), della Costituzione, 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.*

2. *Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e per l'individuazione delle regole tecniche di cui all'articolo 71.*

(2-bis*. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali.*

2-ter*. Le regioni e gli enti locali digitalizzano la loro azione amministrativa e implementano l'utilizzo delle tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese.)*

3*. Lo Stato, ai fini di quanto previsto ai cc. 1 e 2, istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra Amministrazioni di diversa dimensione e collocazione territoriale.*

***3-bis**. Ai fini di quanto previsto ai cc. 1, 2 e 3, è istituita senza nuovi o maggiori oneri per la finanza pubblica, presso la Conferenza unificata, previa delibera della medesima che ne definisce la composizione e le specifiche competenze, una Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali con funzioni istruttorie e consultive.".*

La disposizione richiamata affida alle Regioni ed alle Province autonome un ruolo di guida e coordinamento dell'azione di digitalizzazione dell'azione amministrativa svolta a livello locale e la possibilità per Regioni, Province autonome e enti locali di adottare 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. 50bis del CAD.

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

Il quadro normativo richiamato rafforza, quindi, l'importanza dell'adozione, da parte delle PPAA di soluzioni organizzative e tecniche dirette a garantire la continuità operativa e la sicurezza dei Sistemi Informativi ed affida:

- all'Agenzia per l'Italia Digitale 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 PCO e dei PDR delle Amministrazioni interessate;
  - informare annualmente il Ministro competente;
  - esprimere pareri sugli studi di fattibilità che le Amministrazioni predispongono e sulla base dei quali provvederanno a definire sia il PCO che il PDR.

- alle Amministrazioni centrali, regionali, provinciali e locali, il compito di definire in prima battuta gli studi di fattibilità e sulla base di detti studi (il termine previsto era entro quindici mesi dall'entrata in vigore del D. Lgs. 235/2010) i PCO e i PDR.

- al Ministro competente, il compito di:
  - assicurare l'omogeneità delle soluzioni di CO 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. 50bis 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 PCO e PDR 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 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 PCO e PDR)

Le PPAA 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. 50bis per l'attuazione della CO, 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 artt. 44 e 44 bis del CAD.

Le Amministrazioni devono, una volta acquisito il parere obbligatorio dell'Agenzia per l'Italia Digitale sullo studio di fattibilità tecnica, definire conseguentemente i Piani per descrivere le misure organizzative e tecniche di cui intendono dotarsi per garantire la CO e il DR.

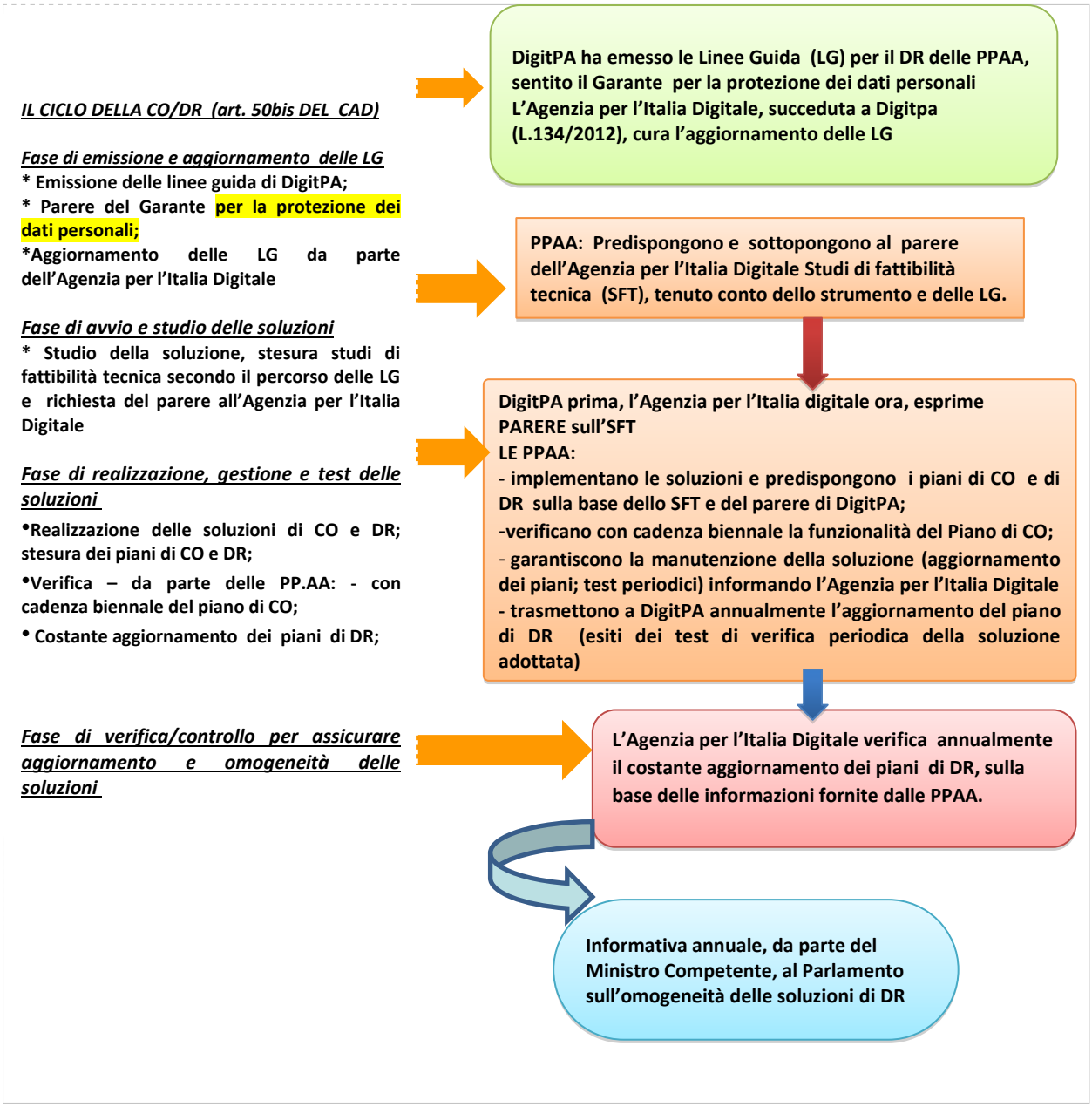
Inoltre, per consentire la verifica annuale del costante aggiornamento dei PDR delle Amministrazioni ai fini dell'informativa annuale prevista dall'art. 50bis, le Amministrazioni dovranno inviare all'Agenzia per l'Italia Digitale, i PDR, nonché verificare le funzionalità dei PCO con cadenza biennale.

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

Ai fini delle attività di verifica attribuite all'AGID, si ritiene opportuno che le Amministrazioni provvedano successivamente anche ad inviare informazioni in merito alle verifiche periodiche effettuate e agli esiti di dette verifiche.

L'omogeneità delle soluzioni indicate in questi piani è assicurata anche attraverso l'informativa annuale al 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 dei principali "attori" coinvolti nell'attuazione degli adempimenti previsti dal richiamato art. 50bis.



2.5 Continuità operativa, Sicurezza dei dati, dei sistemi e delle infrastrutture nel CAD, Sicurezza delle reti e razionalizzazione dei siti e delle infrastrutture digitali

A completare il quadro giuridico ed operativo descritto è necessario ricordare l'art. 51 del CAD, inerente alla "Sicurezza dei dati, dei sistemi e delle infrastrutture delle PPAA".
Il citato articolo, che rimanda alle regole tecniche 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, ha affidato a DigitPA e affida quindi all'Agenzia, 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 PA e l'innovazione il mancato rispetto delle citate regole tecniche parte delle PPAA.

Il secondo c. del richiamato art. 51 conferma altresì, come si è avuto modo di anticipare, che "*I documenti informatici delle PPAA 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*".

Come si è avuto modo di anticipare, il quadro normativo vigente con la L. 134/2012, che ha inteso semplificare e razionalizzare le competenze degli enti che a vario titolo si occupavano dell'ICT e della sicurezza, istituendo l'Agenzia per l'Italia Digitale, rafforza e conferma lo stretto collegamento esistente fra la sicurezza delle reti, dei dati, dei sistemi e delle infrastrutture e l'importanza di adottare soluzione di CO e DR nella gestione dei sistemi informativi automatizzati.

L'Agenzia promuove altresì la definizione e lo sviluppo di grandi progetti strategici di ricerca e innovazione connessi alla realizzazione dell'Agenda digitale italiana in conformità al programma europeo Horizon2020, con l'obiettivo di favorire tra gli altri la sicurezza e gli interventi di razionalizzazione e consolidamento dei data center. Al riguardo, si segnala, fra l'altro, che nel D.L. 179/2012, così come convertito nella legge n. 221/2012 e s.m.i. si prevede espressamente quanto segue:
"Art. 33-septies. Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese
1. L'Agenzia per l'Italia digitale, con l'obiettivo di razionalizzare le risorse e favorire il consolidamento delle infrastrutture digitali delle pubbliche amministrazioni, avvalendosi dei principali soggetti pubblici titolari di banche dati, effettua il censimento dei Centri per l'elaborazione delle informazioni (CED) della pubblica amministrazione, come definiti al comma 2, ed elabora le linee guida, basate sulle principali metriche di efficienza internazionalmente riconosciute, finalizzate alla definizione di un piano triennale di razionalizzazione dei CED delle amministrazioni pubbliche che dovrà portare alla diffusione di standard comuni di interoperabilità, a crescenti livelli di efficienza, di sicurezza e di rapidità nell'erogazione dei servizi ai cittadini e alle imprese.
2. Con il termine CED è da intendere il sito che ospita un impianto informatico atto alla erogazione di servizi interni alle amministrazioni pubbliche e servizi erogati esternamente dalle amministrazioni pubbliche che al minimo comprende apparati di calcolo, apparati di rete per la connessione e apparati di memorizzazione di massa.
3. Dalle attività previste al comma 1 sono esclusi i CED soggetti alla gestione di dati classificati secondo la normativa in materia di tutela amministrativa delle informazioni coperte da segreto di Stato e di quelle classificate nazionali secondo le direttive dell'Autorità nazionale per la sicurezza

(ANS) che esercita le sue funzioni tramite l'Ufficio centrale per la segretezza (UCSe) del Dipartimento delle informazioni per la sicurezza (DIS).
4. Entro il 30 settembre 2013 l'Agenzia per l'Italia digitale trasmette al Presidente del Consiglio dei ministri, dopo adeguata consultazione pubblica, i risultati del censimento effettuato e le linee guida per la razionalizzazione dell'infrastruttura digitale della pubblica amministrazione. Entro i successivi novanta giorni il Governo, con decreto del Presidente del Consiglio dei ministri, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta il piano triennale di razionalizzazione dei CED delle pubbliche amministrazioni di cui al comma 1, aggiornato annualmente.
4-bis. Nell'ambito del piano triennale di cui al comma 4 sono individuati i livelli minimi dei requisiti di sicurezza, di capacità elaborativa e di risparmio energetico dei CED, nonché le modalità di consolidamento e razionalizzazione, ricorrendo ove necessario all'utilizzo dei CED di imprese pubbliche e private nonché di enti locali o di soggetti partecipati da enti locali nel rispetto della legislazione vigente in materia di contratti pubblici.
5. Dall'attuazione del presente articolo non derivano nuovi o maggiori oneri o minori entrate per il bilancio dello Stato".

Nel caso fossero necessarie informazioni per quanto sopra, è possibile inviare la richiesta per le stesse all'indirizzo: "*continuita_operativa@agid.gov.it* ".

Si rimanda altresi alle "*Linee guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione*", disponibili sul sito dell'Agenzia.

2.6 Continuità operativa e dematerializzazione nel CAD

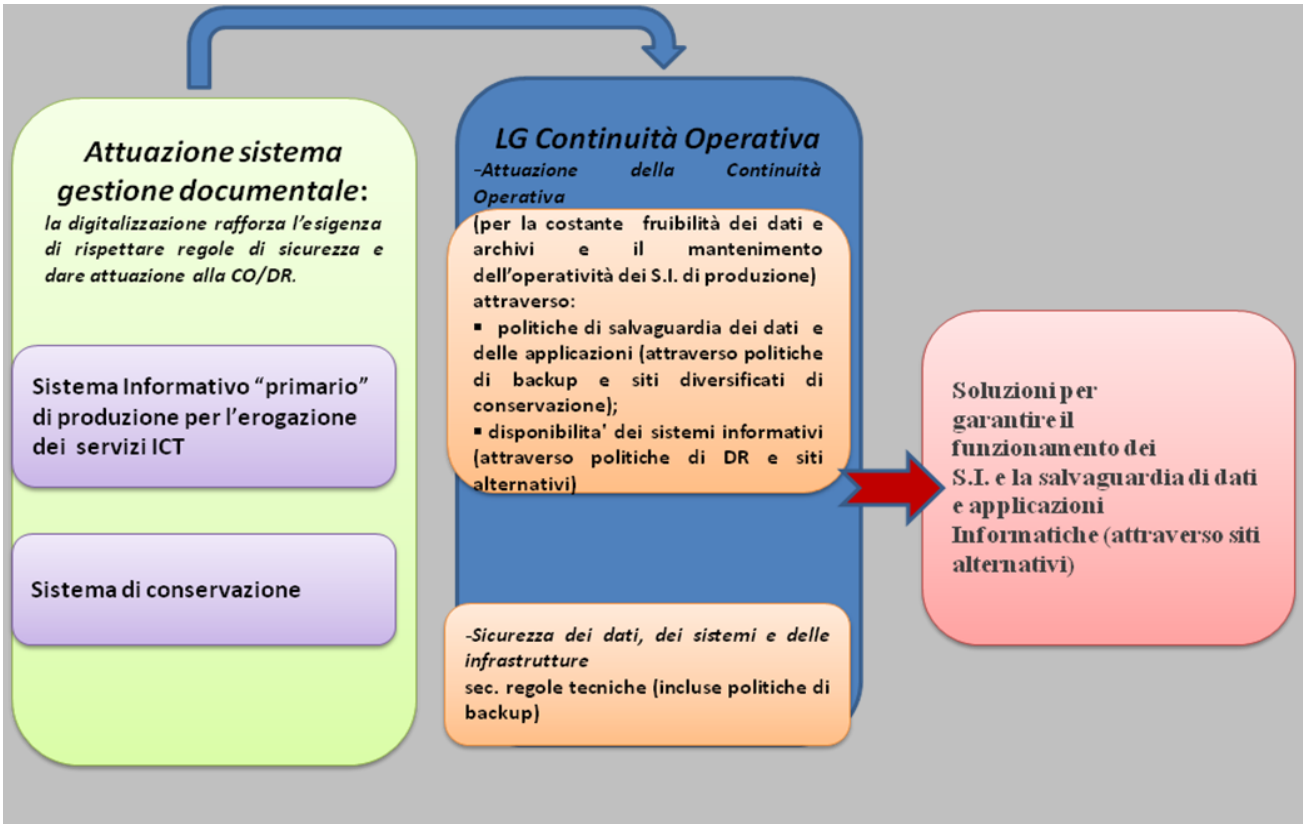
Alla luce di quanto detto non si può non evidenziare la rilevanza strategica che assume l'adozione di soluzioni di CO e di DR, considerando che il CAD impone alle Amministrazioni, fra gli altri, di attivarsi, nel rispetto delle regole tecniche per la gestione informatica dei documenti, per garantire 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, restore e refresh 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. 50bis 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 dei servizi ICT, sia per l'attuazione del sistema di gestione documentale sia per la realizzazione di soluzioni di CO, nel rispetto delle regole tecniche per la gestione documentale e per la sicurezza dei dati, dei sistemi e delle infrastrutture, (cui si rinvia).



Linee Guida sulla Continuità Operativa e il DR applicate alla gestione documentale

2.7 Lo stato di attuazione dell'art. 50bis

Nel periodo di vigenza delle Linee Guida, è stato avviato il percorso di attuazione dell'art. 50bis del CAD e sono stati emessi **circa 800 pareri.**

Da questo primo importante periodo, si rileva che i pareri sono stati richiesti da alcune Amministrazioni Centrali, dalle Regioni, dagli enti locali, dalle università, dalle aziende sanitarie e ospedaliere e da alcuni istituti scolastici.

Nel seguito si riportano sinteticamente le principali evidenze emerse da questo primo anno e mezzo di attuazione del percorso prescritto dall'art. 50bis del CAD.

2.7.1 I servizi tipici di Comuni, Province, Università, ASL e aziende ospedaliere nelle richieste di parere sugli Studi di Fattibilità Tecnica

Nell'individuazione dei servizi da comprendere nella predisposizione dello Studio di fattibilità Tecnica, è emerso quanto segue:

Servizi tipici dei Comuni:

- Gestione atti amministrativi (determine, delibere)
- Gestione Bilancio
- Gestione Economato (inventario, buoni economali)
- Gestione Edilizia
- Gestione Patrimonio
- Gestione Sanzioni, Incidenti, Turni di servizio
- Gestione Protocollo
- Gestione Servizi Sociali
- Gestione SIT (cartografia, civici e toponomastica)
- Gestione sito web
- Gestione Stipendi
- Gestione SUAP
- Gestione Personale (giuridico, presenze)
- Servizi Demografici (anagrafe, CIE, stato civile, elettorale)
- Albo pretorio

Servizi tipici delle Province:

- Affari Generali – Protocollo
- Affari Generali - Ufficio Giunta/Ufficio Consiglio/Gestione atti/Società Partecipate
- Personale - Gestione Economica del Personale
- Personale - Rilevazione presenze
- Gestione Economica dell'Ente - Programmazione Finanziaria
- Gestione Economica dell'Ente - Gestione ordinativi e pagamenti
- Gestione Economica dell'Ente - Controllo di Gestione
- Gestione Economale - Gestione Economato, Ordini e Magazzino
- Sistema bibliotecario della Provincia
- Settore Lavoro - Portale Sintesi
- Gestione Sanzioni Polizia Provinciale
- Rilascio licenze di Pesca
- Gestione venatoria
- Servizio zootecnia, agricolo e dell'alimentazione
- Albo Pretorio
- Siti Istituzionali
- Anagrafe Estesa Sovracomunale
- Sistema Informativo Territoriale
- Servizi provinciali e-gov

Servizi tipici delle Università:

- Consultazione online presenze personale tecnico-amministrativo di Ateneo
- Controllo di gestione
- Customer satisfaction
- Digital signage
- Gestione statistiche
- Portale assistenza rete e servizi di rete
- Portale di cambio password
- Portale Spin-Off
- Produzione Badge
- Affidamenti incarichi attività didattiche
- Albo online
- Consultazione OPAC SBN
- Contabilità integrata di Ateneo
- Dematerializzazione procedimenti amministrativi
- Firma digitale remota docenti
- Gestione giuridico-economica del personale
- Gestione prove di selezione accesso programmato
- Gestione studenti

Servizi tipici delle ASL:

- Esenzione
- Continuità Assistenziale (ex. guardia medica)
- Vaccinazioni
- Scelta e revoca
- Servizio di Prevenzione e Protezione
- Laboratorio di analisi
- Impiantistica e sicurezza sul lavoro
- Patologie cronico degenerative e tumorali
- Medicina legale
- Protesica
- Consultori
- SERT
- Strutture sanitarie accreditate
- Sanità animale
- Servizio igiene degli allevamenti e delle produzioni zootecniche
- Gestione amministrativo-contabile
- Logistica e Supply Chain
- Gestione asset aziendali
- Gestione delle risorse umane
- Servizi direzionali
- CUP diretto e/o centralizzato
- Esposizione referti su FSE

Servizi tipici delle Aziende Ospedaliere:

- servizio di DEA
- servizio di Accettazione/Dismissione e Trasferimento ricoveri (ADT)
- servizio di gestione della Cartella Clinica di ricovero
- servizio di gestione sale operatorie
- servizio di gestione delle terapie intensive
- servizio di gestione ambulatori e casse
- servizio di gestione dei Laboratori Analisi
- servizio di gestione della Radiodiagnostica (Radiologia e Medicina Nucleare)
- servizio di gestione di Anatomia Patologica
- servizio Centro Trasfusionale (SIMT)
- servizio di gestione delle Prenotazioni ambulatoriali (CUP provinciale)
- servizio di gestione del Protocollo e Delibere
- portale Internet
- portale Intranet
- posta Elettronica
- servizio amministrativo contabile e controllo di gestione
- servizio gestione Risorse Umane
- servizio di gestione di Prevenzione e Sicurezza sul Lavoro

Nei vari pareri emessi (da DigitPA e dall'Agenzia) è stato segnalato quanto segue:

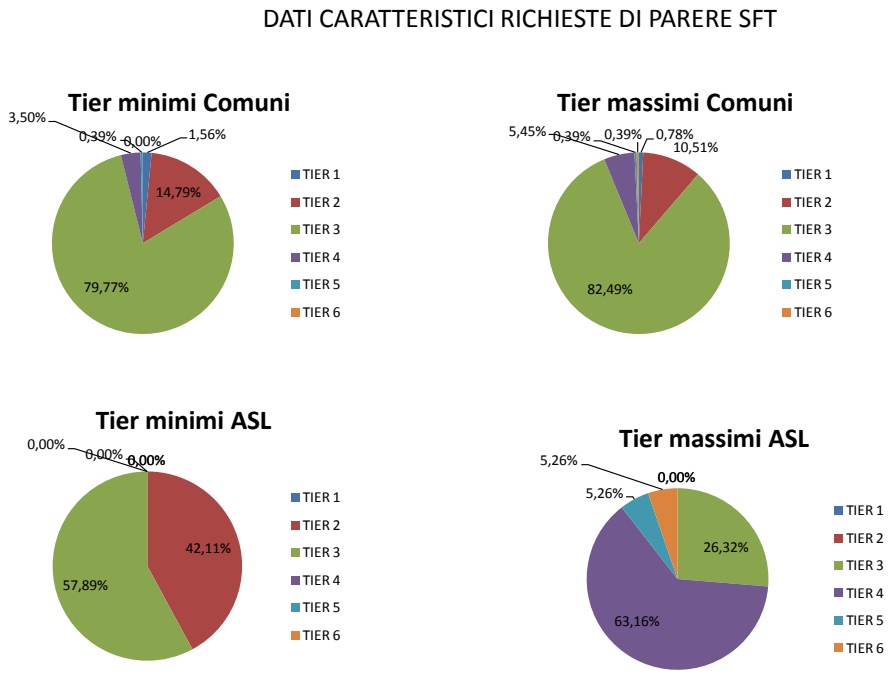
- l'importanza di sottoporre ad autovalutazione i servizi erogati a prescindere se essi siano supportati da servizi applicativi gestiti internamente o forniti da soggetti esterni (aziende, società in house, centri servizi territoriali, altre Amministrazioni ecc.);
- l'opportunità, in taluni casi, di valutare i servizi erogati e non i servizi ICT, applicativi o infrastrutturali, a supporto di questi ultimi, anche se è evidente che le applicazioni e le infrastrutture sulle quali si appoggiano, saranno poi oggetto delle soluzioni di DR; questo in quanto la scelta di valutare direttamente le applicazioni può condurre a valutazioni non sempre coerenti in termini di criticità dei servizi erogati, specialmente in presenza di applicazioni che supportino più servizi;
- l'opportunità di non sottoporre ad autovalutazione servizi/applicazioni infrastrutturali non rivolti agli utenti finali, che non dovrebbero essere oggetto di autovalutazione, in quanto la loro criticità è intrinseca e discende dalla criticità dei servizi/applicazioni supportati (esempi servizi di autenticazione, servizi di rete, ecc.);
- l'opportunità, ove si ritenga necessario valutare comunque i servizi infrastrutturali e/o le applicazioni, che la criticità di questi servizi sia coerente (certamente non inferiore) con quella dei servizi supportati e, al minimo, considerata pari a quella del servizio più critico supportato;
- nel caso in cui sia riscontrata una relazione univoca tra servizio e applicazione (l'applicazione è dedicata all'esercizio di un unico servizio), pur in un quadro di invarianza dei risultati della autovalutazione, si ritiene più opportuno indicare il nome del servizio, in luogo di quello dell'applicazione;
- l'opportunità, relativamente ai servizi non in ambito, di fornire nelle richieste di parere le motivazioni di esclusione: possono essere posti non in ambito servizi che non sono supportati da applicazioni o servizi ritenuti non critici la cui valutazione è rinviata a un momento successivo;
- la necessità, comunque, di porre grande attenzione nella scelta di servizi non in ambito, essendo comunque preferibile una dichiarazione di inclusione futura di un servizio nel perimetro dei servizi protetti, piuttosto che escludere totalmente il servizio da soluzioni di continuità.

2.7.2 Dati statistici ricavati dai pareri (Tier, valori di RTO/RPO attesi)

Si riportano, in via schematica e assolutamente indicativa, alcune informazioni derivanti dai pareri emessi finora, in merito ai valori medi di RPO e RTO (che nei singoli casi possono essere o più bassi o più alti, a seconda della tipologia e criticità dei servizi che entrano nel calcolo di detti valori):

TIPOLOGIA	Numero Servizi in ambito	Numero Classi/servizi valutati	RPO minimo (h)	RPO Massimo (h)	RTO minimo (h)	RTO Massimo (h)
Università	21	14	8,26	60,87	12,29	87,27
Comune	22	9	28,09	45,32	37,81	73,47
Asl	26	6	16,42	70,95	11,71	91,16
Regione	95	10	0,67	120,00	3,00	136,00
Provincia	25	10	12,44	42,67	26,67	88,00

I Tier prevalentemente individuati sono di seguito schematicamente descritti:



Dall'esperienza maturata nelle fasi di emissione dei pareri ai sensi dell'art. 50bis, c. 4 del CAD emerge, in via esemplificativa e non esaustiva, che le Amministrazioni che si sono sottoposte al parere, per adottare i Tier suggeriti dallo strumento di autovalutazione, hanno inteso percorrere le seguenti soluzioni di DR:

- Tier 1 per istituti scolastici con 1 server e 10 PDL, con trasferimento settimanale dei supporti dati in sede secondaria o di altro istituto e accordo con il fornitore per installazione server in caso emergenza,

- Soluzioni Tier 3 per piccoli e medi comuni con collegamento fra le sedi del sito primario e secondario tramite VPN, su rete SPC e con vincoli di RPO pari al massimo a 1 giorno e RTO da 1g. a 3 gg.;

- Soluzione Tier 4 tra due sedi della stessa amministrazione (piccolo o medio comune) con piattaforme virtualizzate;

- Soluzione di CO a livello di campus per Università o azienda ospedaliera e sito per DR geografico presso fornitore esterno (eventuale società regionale o consorzio) o altra amministrazione (mutuo soccorso);

- Grande comune o regione: gara per individuazione di un fornitore esterno cui affidare la realizzazione e gestione di un sito alternativo e dei servizi di DR (a volte inclusi servizi di connettività) con Tier differenziati;

- Amministrazioni centrali in full outsourcing che hanno rivisto le criticità dei servizi, rinegoziato i requisiti di DR e integrato i propri piani e le strutture organizzative di CO e DR con quelle dei fornitori.

2.7.3 Le principali criticità e raccomandazioni nei pareri resi dall'Agenzia

Per quanto attiene alle principali criticità emerse si osserva quanto segue.
Prevalentemente a causa delle problematiche di carattere finanziario che hanno caratterizzato in generale l'operato di tutti gli ambiti della PA centrale e locale ma anche per problemi di carattere organizzativo, quasi nessuna delle Amministrazioni ha potuto ottemperare provvedendo a dotarsi dei PCO e dei PDR entro il 25 aprile 2012, come avrebbe richiesto l'art. 57 del D. Lgs. 235/2010 (che ha innovato sul punto il CAD).

In questo periodo di prima attuazione del percorso descritto dall'art. 50bis, sono state, in linea di massima, evidenziate le seguenti principali criticità:

- vincoli di budget;
- necessità di interventi di razionalizzazione sui siti primari (consolidamento, virtualizzazione,…) prima di adottare soluzioni di DR;
- difficoltà nell'individuazione e comprensione dei ruoli e attività del Responsabile della CO;
- mancanza delle necessarie competenze tecniche non sempre presenti, specialmente nelle Amministrazioni di piccole dimensioni;
- difficoltà nell'armonizzazione delle liste dei servizi e delle valutazioni di criticità per stessa tipologia di Amministrazione;
- rischio di moltiplicazione dei data center in assenza di soluzioni condivise.

In merito al rischio di moltiplicazione dei data center, si segnala che sia nei pareri resi ai sensi dell'art 50 bis che nei pareri resi ai sensi del D.lgs. 177/2009 e della legge 134/2012 e s.m.i. l'Agenzia già raccomanda quanto segue:

- per quanto attiene alle Publiche Amministrazioni Centrali e agli Enti Pubblici non Economici:
  - l'invito ad attivarsi per effettuare e mantenere sempre aggiornato un adeguato assessment dei propri sistemi, per garantire l'adozione di soluzioni di DR e il loro costante monitoraggio e aggiornamento per i sistemi e applicazioni necessari per l'operatività e le funzioni istituzionali, anche verificando presso l'Agenzia per l'Italia Digitale le condizioni che possano portare a differenti soluzioni che tengano conto del consolidamento e della razionalizzazione dei CED della PA conseguenti a quanto disposto dall'art. 33-septies del D.L. 179 convertito nella legge 221/2012;
  - l'invito, ove si riscontrasse che ancora non è stato richiesto parere ai sensi dell'art. 50 bis, a predisporre lo studio di fattibilità tecnica e della soluzione/delle soluzioni di DR, tenuto conto di quanto disposto dal C.A.D. e s.m.i. e del disposto del citato art. 33-septies che mira a orientare le Amministrazioni nella scelta di soluzioni che consentano il più possibile, di razionalizzare i siti da gestire e conseguire risparmi e maggiore efficienza nella gestione dei sistemi ICT, al fine di incrementare l'efficienza, ottenere riduzioni di spesa e migliorare la qualità dei servizi offerti (come del resto già accaduto e sta accadendo in altri Paesi europei);
- per quanto attiene alle Amministrazioni e enti locali (solo pareri art. 50 bis CAD): l'invito, prima di dare seguito all'avviamento delle attività per la realizzazione della soluzione, a verificare presso la propria Regione la presenza di piani regionali conseguenti a quanto disposto dall'art. 33-septies del D.L. 179 convertito nella legge 221/2012.

Nel caso fossero necessarie informazioni per quanto sopra, è possibile inviare la richiesta per le stesse all'indirizzo: "*continuita_operativa@agid.gov.it* ".

L'Agenzia per l'Italia Digitale ha svolto e svolge azioni parallele all'emissione dei prescritti pareri, sia diffondendo le informazioni utili all'attuazione della continuità operativa sia supportando le Amministrazioni nella fase di richiesta del parere e di elaborazione dello Studio di Fattibilità Tecnica, nonché più in generale nell'individuazione della soluzione tecnica più adeguata e nel superamento progressivo delle varie criticità segnalate.

Come previsto dai pareri emessi e dalla circolare 58/2011, l'Agenzia è in attesa di ricevere rispetto ai pareri emessi i PCO e PDR, nonché evidenze in merito all'adeguamento alle eventuali condizioni espresse nei pareri, al fine di predisporre la Relazione sullo stato di attuazione dell'art. 50bis al Ministro competente, essenziali ai fini dell'avvio delle attività di monitoraggio e verifica delle soluzioni di DR.

Il costante processo di emissione dei pareri e la ricezione e verifica dei Piani richiamati, il monitoraggio e la verifica dei livelli di aggiornamento delle soluzioni, contribuirà in futuro sia a tenere sotto controllo lo stato delle iniziative di attuazione della CO e delle soluzioni di DR, sia a migliorare le azioni che l'Agenzia intende porre in essere a supporto delle Amministrazioni che sono chiamate a dare attuazione all'art. 50bis.

3 INFRASTRUTTURE E ORGANIZZAZIONE IT PER LA CONTINUITÀ OPERATIVA

Nel presente capitolo vengono fornite indicazioni sulle infrastrutture, con particolare riferimento ai Data Center, e sull'organizzazione da adottare per l'attuazione di soluzioni di CO e di DR.

3.1 Infrastrutture e sistemi: Cenni ai data center della PA

E' necessario ribadire che sul tema dei Data Center l'Agenzia, come richiamato al capitolo 2, è stata investita da importanti attività volte alla razionalizzazione in ambito pubblica amministrazione, che verranno approfondite in altri contesti. Nel contesto attuale, invece, quello delle soluzioni di Disaster Recovery, questo paragrafo del capitolo 3 ha la sola finalità di introdurre alcuni elementi atti a rendere le Amministrazioni coscienti delle caratteristiche che un Data Center dovrebbe comunque avere anche se utilizzato per attività di Disaster Recovery.

Quale precisazione preliminare, si sottolinea che, nell'ambito delle presenti Linee Guida, si utilizzerà l'espressione "Data Center" come sinonimo del termine "CED", utilizzato nella ricordata norma al capitolo 2, nella considerazione che l'espressione "Data Center" trova diffuso riscontro nella letteratura nazionale e internazionale sul tema.

Infine, va sottolineato come il modello di riferimento nell'ambito dei Data Center della pubblica amministrazione è costituito dallo standard TIA-942 (versione del 2010), che definisce 4 livelli ("Tier") rappresentanti progressive e più stringenti caratteristiche di un Data Center.

Nel seguito, a puro titolo introduttivo del tema, si fornirà una classificazione semplicemente discorsiva dei Data Center, rimandando al citato standard TIA-942 per definizioni formali e dettagliate.

3.1.1. Definizione di Data Center

Per Data Center (nel seguito DC) si intende una struttura fisica, normalmente un edificio compartimentato, unitamente a tutti gli impianti elettrici, di condizionamento, di attestazioni di rete, di cablaggi, ecc. e a sistemi di sicurezza fisica e logica, che in tale edificio sono presenti, progettato e allestito per ospitare e gestire un numero elevato di apparecchiature e infrastrutture informatiche e i dati ivi contenuti, allo scopo di garantirne la sicurezza fisica e gestionale.

Una possibile classificazione dei DC è la seguente:

- **Server Cabinet:**
  in questo caso ci si riferisce a locale molto piccolo o anche semplicemente un armadio, talvolta non sotto il controllo dell'IT, con caratteristiche di sicurezza e di impianti di raffreddamento molto ridotte o nulle; il locale ha una superficie di solito sotto i 10 metri quadri e ospita di solito meno di 5 server; la potenza utilizzata è nell'ordine dei 2 kW.

- **Server Room:**
  in questo caso il riferimento è a un locale dedicato ai computer, solitamente sotto il controllo dell'IT, di dimensioni di circa 20 metri quadri; che può essere dotato di impianti di alimentazione e di raffreddamento dedicati, come pure di infrastrutture di sicurezza; ospita tipicamente tra i 5 e i 20 server; la potenza utilizzata è nell'ordine di 10-15 kW.

- **Data center "small":**
  può essere una locale con una superficie fino a 150 metri quadri; dispone di controllo degli accessi tramite badge o codice pin; ha sistemi di alimentazione e di raffreddamento ridondati per garantire valori di temperatura e umidità costanti; ospita tipicamente fino a 150 server; la potenza utilizzata è nell'ordine di 100 kW.

- **Data center "mid-Tier":**
  può ospitare fino a 600 server, su una superficie fino a 600 metri quadrati. Dispone di sistemi di raffreddamento di fascia alta e ridondati ed è generalmente protetto da 2 livelli di protezione, fisica e logica; la potenza utilizzata può raggiungere i 500-600 kW.

- **Data center "enterprise":**
  in questo caso, le dimensioni del data center, che può ospitare anche 6.000 server, possono raggiungere 6.000 metri quadri; dispone di sistemi di raffreddamento avanzati e di alimentazione ridondata, con protezione dell'accesso sia fisica, sia logica; la potenza utilizzata può superare 5.500 kW.

Le indicazioni che sono di seguito rappresentate, pur avendo valore generale, sono particolarmente applicabili a Data Center inquadrabili come "mid-Tier" ed "enterprise".

3.1.2 Localizzazione

I principali fattori che devono essere valutati nella scelta della localizzazione di un DC sono i seguenti:

- attenta valutazione delle caratteristiche della localizzazione del sito per rendere minime potenziali situazioni di alluvioni, terremoti, frane ecc.[2]; deve anche essere attentamente valutata la condizione climatica complessiva (temperatura/umidità): luoghi con basse temperature e umidità possono consentire risparmi energetici;
- densità della rete elettrica distributiva e dei suoi punti di accesso; la progettazione di un DC in aree a bassa densità abitativa aumenta i costi delle infrastrutture dedicate per allacciarsi alla rete, date le potenze richieste per questi contratti di fornitura, anche se i costi di acquisizione dei terreni potrebbero risultare più convenienti proprio in queste aree;
- disponibilità di infrastrutture per le telecomunicazioni, preferibilmente a livello di backbone; le aree a ridosso dei grandi centri metropolitani, quali Roma, Milano, Napoli, sono da preferire visto la sempre più crescente disponibilità di reti MAN in fibra ottica; nel caso delle PA, laddove possibile, è utile integrare il DC nella connettività della rete SPC e di altre reti convenzionate con le PA;
- impatto del fattore "distanza" relativamente alle performance dei servizi erogati per soluzione di continuità operativa; allo stato attuale delle reti di telecomunicazioni e delle tecnologie applicate su queste reti, il problema della distanza tra l'utilizzatore (amministrazione) e il DC non è da sottovalutare; la distanza massima sostenibile va dimensionata sulla base dell'architettura e della modalità di sincronizzazione dei dati a supporto delle attività di CO, tenendo conto che la distanza può influire sul costo del collegamento;

[2] Al proposito, è possibile trovare utili indicazioni nel documento "I SERVIZI MINIMI ESSENZIALI PER L'ADOZIONE DELLE SOLUZIONI DI DISASTER RECOVERY" reperibile al link: http://www.digitpa.gov.it/sites/default/files/Raccomandazioni_PROFILI%20MINIMI%20SERVIZI%20DI%20DR_v_2_4_0.pdf

- localizzazione del sito preferibilmente su territorio nazionale, se non in contrasto con la normativa sugli appalti.

3.1.3 Spazi dedicati al DC

Le parti di cui si compone un DC si possono classificare, sinteticamente, in:

- Sistemi di raffreddamento: gruppi frigo, pompe e ventole in grado di supportare un canale di refrigerazione a doppio anello e con varie possibilità di sezionamento.
- Sistemi di approvvigionamento energetico: tipicamente l'infrastruttura comprende il collegamento con la rete elettrica, generatori, batterie di backup e l'energia per il sistema di raffreddamento.
- IT equipment: contiene gli apparati elettronici che sono utilizzati per l'elaborazione dei dati (server), l'immagazzinamento dei dati (storage) e le comunicazioni (network).

Tutti i locali di un DC devono essere conformi a quanto previsto dalle attuali norme sulla sicurezza e salute sul luogo di lavoro dei lavoratori, di cui al d.lgs. n. 81/2008 e successive modificazioni.

3.2 Caratteristiche strutturali del DC

3.2.1.Pavimenti e solai

I solai di un DC dovrebbero essere certificati per sostenere una pressione statica massima, misurata in riferimento sia alla superficie di appoggio distribuito sia a quella di appoggio puntiforme.
E' possibile, comunque, che nella vita utile di un DC si possano verificare eventi che richiedono delle operazioni di rinforzo dei solai, quali:

- spostamento delle macchine installate per esigenze operative o incidentali;
- installazione di apparati non rackable di peso eccezionale per cui è richiesta una progettazione ad-hoc.

3.2.2. Sistemi di illuminazione

In accordo alle linee guida emesse dall'ENEA[3] in merito alla progettazione di DC, nella progettazione dell'impianto elettrico del data center si dovrà considerare anche la parte relativa all'illuminazione. Le lampade, infatti, contribuiranno ad aumentare il carico termico da dissipare nella sala. In questo caso è consigliato l'uso di tecnologie di illuminazione efficienti, come per esempio i led, abbinati ad un sistema di controllo automatico che accenda l'impianto solo quando è necessario e consenta l'illuminazione di aree specifiche nei grandi centri.

3.2.3 Cablaggi e telecomunicazioni

La topologia di cablaggio di un DC è di solito progettata conformemente allo standard definito dalla Telecommunications Industry Association. La normativa denominata TIA-942 regola la progettazione delle infrastrutture di telecomunicazione e le tipologie di cablaggio dei DC.

[3] https://www.google.com/url?q=http://www.enea.it/it/Ricerca_sviluppo/documenti/ricerca-di-sistema-elettrico/elettrotecnologie/5-linee-guida-datacenter-07.09.2010.pdf&sa=U&ei=81nAUN7MMcXBhAftpIHQDg&ved=0CAcQFjAA&client=internal-uds-cse&usg=AFQjCNGd-X9yK1G7EGbP-JrZk1mjoVPUPA

3.2.4 Armadi rack e cage

I rack sono armadi costruiti ai fini di permettere l'alloggiamento di server, nel pieno rispetto degli standard di alloggiamento e di alimentazione elettrica e dissipazione termica del DC. Le dimensioni massime dei server installabili fanno riferimento alle dimensioni interne nette dei rack.
E' possibile creare delle strutture ad hoc per la compartimentazione di una superficie dedicata all'interno della sala, definite cage, delimitate da pareti grigliate; la predisposizione di una cage consente di gestire l'accesso esclusivo alla zona compartimentata, anche tramite un lettore badge, consentendo gli accessi allo staff addetto oltre che al personale preposto alle pulizie, alla manutenzione ed alla vigilanza e di monitorare tali accessi.
La struttura di parte grigliata utilizzata per la compartimentazione, consente sia di avere un grado di sicurezza maggiore di un ambiente condiviso in un contesto comunque di elevata sorveglianza, sia di sfruttare correttamente/completamente l'impianto di raffreddamento del DC, garantendo il passaggio dell'aria ed evitando microclimi.

3.2.5 Sistemi di raffreddamento e climatizzazione

L'analisi e la valutazione dei sistemi di raffreddamento di un DC contribuisce a garantire la continuità del servizio del cliente. Le prestazioni degli apparati IT sono fortemente influenzate dalle condizioni ambientali e in particolare dalle variazioni di temperatura o umidità, fino ad arrivare, nel caso peggiore, all'interruzione del servizio.
Una dettagliata descrizione dei parametri tecnici a supporto di una valutazione oggettiva di tali sistemi all'interno di un DC non è proponibile in quanto deve tener conto di fattori quali:

- tecnologia a supporto delle infrastrutture informatiche;
- sistema di riferimento per la misurazione della quantità di calore prodotta (BTU, Watt, tonnellate al giorno);
- individuazione delle altre fonti di calore all'interno del DC.

Pertanto, in linea del tutto generale, possiamo classificare i requisiti che i sistemi di raffreddamento dovrebbero soddisfare in:

- Requisiti funzionali:
    - temperatura ambiente compresa tra 22 e 25° C;
    - percentuale di umidità compresa tra il 30 ed il 70%;
    - temperatura costante in ogni compartimento e fra le diverse parti di ogni rack.
- Requisiti non funzionali:
    - scalabilità e adattabilità: i sistemi di raffreddamento sono di solito sovradimensionati per far fronte a ogni possibile esigenza futura; un potenziamento della capacità di raffreddamento successivo all'installazione del sistema risulterebbe estremamente complesso;
    - semplificazione: i sistemi di raffreddamento complessi sono più suscettibili a interruzioni del servizio;
    - affidabilità: sono necessarie soluzioni di condizionamento ridondanti e di supporto al sistema principale;
    - uniformità: il disaccoppiamento fra componente IT installata nel DC e sistema di raffreddamento dovrebbe essere quanto più avanzato possibile; l'installazione tipica di un DC comprende generalmente unità di diverse tecnologie, per cui un'eventuale personalizzazione del sistema di raffreddamento a fronte dell'introduzione di nuovi dispositivi IT potrebbe essere dispendiosa nei tempi e nei costi;
    - gestione: la gestione degli impianti di raffreddamento dovrebbe essere affidata a delle sale di controllo automatizzate.

3.2.6 Sistemi di alimentazione e di continuità elettrica

3.2.6.1 Sistema di distribuzione dell'energia

Il sistema di distribuzione dell'energia di un DC va dimensionato tenendo conto dei consumi in potenza del sistema di raffreddamento, della componente IT e degli apparati a supporto del sistema di alimentazione elettrica principale. In molti casi si procede al sovradimensionamento nella previsione di estensioni future. Il requisito più stringente richiesto a un DC che supporti l'attività di CO e di DR è di garantire un sistema di generazione e distribuzione dell'energia ridondato. La logica di ridondanza si deve avvalere di apparecchiature quali UPS, batterie tampone, gruppi elettrogeni a garanzia della continuità di erogazione a fronte di guasti della rete di distribuzione primaria. Per il completamento della ridondanza dell'alimentazione elettrica anche per i server mono-alimentati, su base progettuale e al fine di aumentare i livelli di servizio desiderati, è possibile inoltre installare sui rack degli switch di corrente STS (Source Transfer Switch). Con tali apparati i server mono-presa (e dunque mono-alimentati) possono fruire dell'alimentazione da una presa o da un'altra, nel caso in cui una delle due sia fuori servizio. Il transitorio della fase di commutazione da un'alimentazione all'altra deve essere limitato e ben definito.

3.2.6.2 Distribuzione dell'energia: rete di terra/UPS/gruppi elettrogeni

I gruppi di continuità (UPS) devono essere configurati in almeno due catene in formazione ridondata. Gli UPS devono garantire la continuità della componente IT e del sistema di raffreddamento.

Le batterie tampone devono poter garantire in autonomia l'erogazione dell'alimentazione per almeno un tempo pari all'attivazione, a regime, dei gruppi elettrogeni o al ripristino del sistema primario.

I gruppi elettrogeni intervengono nel caso in cui le interruzioni superano un certo livello di criticità e/o un limite temporale definito. In questo caso va stabilito anche un piano di approvvigionamento alternativo per garantire la continuità di erogazione degli stessi (es. carburante).

3.2.6.3 Efficienza energetica

Non è possibile fare riferimento ai componenti energetici di un DC senza accennare al tema dell'efficienza energetica.

Come è noto, l'indicatore di efficienza energetica più diffuso e utilizzato è il PUE (*Power Usage Effectiveness*) che rappresenta il rapporto tra il consumo energetico totale di un DC e quello relativo alla sola componente IT. Più il PUE è alto, meno efficiente è il DC sotto il profilo energetico. E' auspicabile, da questo punto di vista, l'adozione delle nuove tecnologie dette "*green data center*". Sono tecnologie che consentono la riduzione dei consumi energetici dei data center, attraverso l'installazione di "isole" – unità modulari ad alta efficienza energetica dotate di impianti di condizionamento autonomi e integrati – che permettono di evitare il condizionamento dell'intero ambiente, dove sono ospitati gli elaboratori, limitandosi a condizionare le sole "isole". Consentono, tra l'altro, di diminuire i tempi di installazione di nuovi apparati.

3.2.7 Sistemi antincendio e antiallagamento

Le caratteristiche di sicurezza di un DC devono mirare alla riduzione dei rischi per le persone e per scongiurare eventuali manomissioni sui sistemi interni.

In linea con quanto previsto dalle leggi e normative vigenti, i sistemi antincendio devono poter garantire la sicurezza negli ambienti a uso tecnologico e non. Pertanto, oltre al piano antincendio con mezzi estinguenti mobili e idranti, è opportuno che i DC fossero provvisti di una centrale del

sistema di rilevazione incendi in grado di coordinare e gestire automaticamente la sensoristica di rilevazione fumi e spegnimento.

Le sale tecnologiche dei DC dovrebbero essere dotate di un sistema antiallagamento sottopavimento attivato tramite rilevazione sensoristica.

3.2.8 Protezione del Data Center

Tra le misure di sicurezza poste a protezione del Data Center si ricordano:

- **Perimetro di sicurezza esterno:**
  - recinzione perimetrale che delimita il confine di proprietà composta da una protezione passiva anti scavalcamento;
  - aree esterne monitorate da barriere infrarossi e/o sistemi di videoanalisi e sistemi di videosorveglianza con videoregistrazione;
  - accesso pedonale selettivo/singolo;
  - accesso veicolare selettivo;
  - ronda armata.
- **Perimetro di sicurezza interno**
  - presidio di vigilanza per controlli aree interne ed esterne, supervisione allarmi, gestione visitatori con consegna badge in osservanza a disposizioni aziendali e specifiche per i DC;
  - presidio di reception per la gestione degli accessi;
  - tornelli a braccio triplice prospicienti al locale del presidio vigilanza e reception.
- **Perimetro di massima sicurezza interno**
  - varco di accesso sala sistemi dotato di protezione passiva interbloccato;
  - sistema di controllo accessi con gestione delle liste abilitati ;
  - sensori magnetici stato porta in grado di rilevare lo stato della porta;
  - uscite d'emergenza dotate di sensori stato porta.
- **Protezioni procedurali**
  - identificazione visiva personale a mezzo nastri porta badge di identificazione;
  - procedura accesso al Data center.

3.2.9 Controllo delle infrastrutture

Un sistema di supervisione è necessario per il monitoraggio degli impianti industriali (meccanico ed elettrico), la rilevazione della temperatura e dell'umidità di sala.

Il monitoraggio deve avvenire preferibilmente tramite due postazioni, una allocata presso i servizi di manutenzione impianti e l'altra presso il presidio dei DC.

Tali postazioni oltre a mostrare l'andamento degli impianti in tempo reale, forniscono la segnalazione di eventuali anomalie di funzionamento e l'andamento delle variabili ambientali di temperatura ed umidità.

Gli operatori vengono avvisati delle anomalie non solo mediante segnalazione a monitor ma anche con segnalazione acustica e per gli eventi più gravi via sms verso i cellulari di servizio.

Con adeguato software a corredo è possibile tracciare tutti gli interventi e fornire statistiche e dati di trend di qualsiasi variabile controllata.

Gli impianti da controllare sono:

- cabina elettrica di ricevimento MT;
- cabina elettrica di trasformazione MT/bt;
- quadri elettrici (generali bt, generale continuità A+B, sale sistemi);
- UPS;
- trasformatori MT/bt;
- condizionatori sale sistemi;
- gruppi Frigo;
- gruppi Elettrogeni;
- elettropompe impianto ad acqua refrigerata;
- multimetri;
- sonde di temperatura e umidità.

E' inoltre anche preferibile che un servizio di presidio impianti tecnologici offra una copertura h24/365 giorni annui per supporto a fronte di eventuali fault impiantistici.

3.3 I processi gestionali

3.3.3 Gestione operativa, controllo delle prestazioni e manutenzione programmata

La gestione operativa è svolta a livello software indipendentemente dalle infrastrutture sottostanti da controllare. L'astrazione di sistemi eterogenei tramite software gestionali consente di impostare le proprie policy e procedure per la gestione del DC senza tener conto dei vincoli generalmente associati alle soluzioni basate su un unico fornitore. La standardizzazione del software di gestione, inoltre, ha come obiettivi:

- il miglioramento dell'efficienza operativa degli impianti;
- il controllo e ottimizzazione dei consumi;
- il controllo delle prestazioni degli impianti;
- le attività di manutenzione programmata;

Nel particolare, si stanno affermando soluzioni centralizzate e standard di monitoraggio e gestione dei sistemi critici di un DC. Inoltre, tali sistemi devono garantire nella fase di monitoraggio l'approvvigionamento dei dati operativi (temperatura, consumi di energia, raffreddamento) ed informatici (utilizzo di risorse CPU, dischi, rete, memoria) necessari a redigere i piani di manutenzione programmata.

3.3.4 Gestione della configurazione, delle capacità e dei processi di approvvigionamento

I sistemi devono essere in grado anche di supportare attività di *intelligent capacity planning*.
Il dimensionamento dell'infrastrutture DC avviene nella fase di progettazione sulla base di informazioni e requisiti ben definiti. Successivamente, la modifica delle capacità viene pianificata in base ai risultati dell'analisi predittiva condotta su determinati KPI.

Nell'ambito delle soluzioni di CO/DR, il sito secondario deve gestire e dimensionare le proprie risorse attraverso una configurazione flessibile, dinamica e tempestiva in ottemperanza ai workload che si possono avere in caso di disastro:

- scalabilità attraverso l'avvio di nuove macchine fisiche o virtuali;
- upgrade nell'approvvigionamento di energia elettrica e della rete di telecomunicazione;
- dimensionamento del sistema di raffreddamento in base alla richiesta reale dei server.

La riconfigurazione delle risorse in caso di DR è vincolata ai tempi di ripristino definiti negli LDS. In tale contesto si inseriscono le tecniche di virtualizzazione in cui le macchine virtuali possono essere dimensionate dinamicamente a tempo di esecuzione.

3.3.5 Processi di approvvigionamento

I processi di approvvigionamento possono essere regolamentati dalla norma ISO 9001:2008, anche se non deve necessariamente essere richiesta una certificazione di qualità per tale aspetto. In ogni caso, relativamente all'approvvigionamento delle materie prime quali energia, connettività, IT equipment, carburante per i generatori ecc. è fondamentale la pianificazione.

E' opportuno identificare e stimare i tempi e i rischi legati ai singoli fornitori per poter intervenire adeguatamente a seconda dei casi. Inoltre, i DC dovranno attivare dei piani di approvvigionamento alternativi per garantire la continuità operativa del cliente in seguito ad interruzioni o ritardi della rete di fornitura principale.

3.4 LDS del Data Center

Premesso che le presenti Linee Guida riportano una adeguata varietà di esempi di LDS applicabili alla prestazione di un servizio di DR, nel presente paragrafo vengono presentati ulteriori esempi di livelli di servizio relativi a infrastrutture DC particolarmente indicati per gli aspetti di alimentazione elettrica, distinti per apparati dotati di doppia alimentazione e per apparati non dotati di doppia alimentazione per i quali sia previsto l'utilizzo o meno di un STS, per le componenti meccaniche del DC e per alcuni aspetti della sicurezza fisica dello stesso DC.

3.4.3 Gestione impiantistica industriale – parte elettrica

Parametri Prestazionali	LDS di riferimento
Disponibilità annua per apparati con doppia alimentazione.	99,98%.
Disponibilità annua per apparati non dotati di doppia alimentazione per i quali si sia utilizzato un STS (Source Transfer Switch).	99,7 %.
Disponibilità annua per apparati non dotati di doppia alimentazione	99,5 %.
Continuità operativa in caso di black-out alimentazione da cabina primaria.	I sistemi di continuità UPS garantiscono l'alimentazione senza interruzione agli apparati mediante le batterie, per il tempo necessario all'avvio ed inserimento sull'impianto dei GE tramite sistema di commutazione automatica, operazione che si compie nel giro di alcuni minuti (di norma entro 5 minuti al massimo)
Tempo di intervento in caso di guasto	Entro 4 ore
Tempo ripristino guasti	Entro 8 ore dall'inizio dell'intervento

3.4.4 Gestione impiantistica industriale – parte meccanica

Parametri Prestazionali	LDS di riferimento
Disponibilità annua	99,7%
Tempo di intervento in caso di guasto	Entro 4 ore
Tempo ripristino guasti	Entro 8 ore dall'inizio dell'intervento
Condizioni ambientali garantite nelle sale dati	Estate/Inverno Temperatura corridoi freddi: ≤ 24+1°C Umidità relativa: 30%< HR < 70% Ricambi d'aria pari ad un minimo di 1,5 volumi/ora

3.4.5 Gestione Sicurezza Fisica

Parametri Prestazionali	LDS di riferimento
Presidio guardiania	on site h24
Conservazioni immagini registrate e tipo di supporto	Se attivato il servizio, 24 ore di latenza su supporto digitale
Tempi intervento in caso di allarmi	Immediato considerando il presidio on site

3.4.6 Certificazioni

E' fortemente raccomandabile che il DC sia in possesso delle seguenti certificazioni di qualità riferite all'infrastruttura ed ai processi:

- ISO 27001:2005
- ISO 9001:2008

L'eventuale presenza della certificazione ISO 20000 rappresenta un'ulteriore garanzia.

3.5 Strutture per la gestione dell'emergenza: coinvolgimento e ruolo dei vertici dell'amministrazione

Nel prosieguo vengono fornite indicazioni sull'organizzazione da adottare per l'attuazione di soluzioni di CO e di DR con riferimento al Responsabile CO e al Comitato di Crisi.

3.5.3 Descrizione caratteristiche e compiti responsabile CO

Il ruolo del responsabile della Continuità Operativa è quello di supportare l'Amministrazione per predisporre tutte le misure necessarie per ridurre l'impatto di un'emergenza ICT e reagire prontamente e in maniera efficace in caso di una interruzione delle funzioni ICT, a supporto dei servizi erogati, dovuta a un disastro. Inoltre ha la responsabilità' di sviluppare e mantenere aggiornato il PCO.

Il Responsabile della Continuità Operativa e' membro del Comitato di crisi.
I compiti fondamentali di cui il responsabile della Continuità Operativa si deve far carico, direttamente o indirettamente, durante la **condizione di normalità operativa dell'ICT** sono:

- predisporre o coordinare la predisposizione dello Studio di Fattibilità Tecnica e della relazione sullo stato di attuazione del CAD;
- curare l'invio della richiesta di parere secondo le modalità previste dalla circolare n. 58;

- mantenere i rapporti con l'Agenzia Italia Digitale, in particolare per gli adempimenti relativi al SFT ed agli aggiornamenti periodici del PCO e del PDR;
- interagire con i diversi settori dell'Amministrazione per individuare le migliori soluzioni tecniche, procedurali e organizzative da implementare nel PCO;
- sviluppare e mantenere aggiornato il PCO e il PDR;
- pianificare e coordinare i test di Continuità Operativa e produrre la reportistica necessaria;
- collaborare con i servizi ICT per aggiornare le procedure tecniche e verificare il corretto funzionamento dei sistemi di disaster recovery;
- assicurare che i percorsi formativi per il personale coinvolto nelle attività di ripristino e rientro descritte nel PCO siano opportunamente seguiti;
- avviare un processo di valutazione di impatto sul PCO, per i cambiamenti tecnici e organizzativi che coinvolgono l'Amministrazione.

Relativamente alle situazioni che possono portare alla condizione di **stato di emergenza ICT**, il responsabile della Continuità Operativa, oltre ad avere un ruolo fondamentale nella gestione dell'emergenza ICT, è impegnato in tutte le attività necessarie che devono essere svolte o coordinate direttamente da questa figura:

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

Qualora la situazione di emergenza ICT si prolunghi oltre quanto previsto e concordato con le altre strutture dell'amministrazione che erogano servizi critici usando funzioni ICT, il responsabile della Continuità Operativa deve rapportarsi con il responsabile della Continuità Operativa generale dell'amministrazione, se presente, per valutare le azioni gestionali/comunicative, amministrative più opportune

3.5.4 Strutture per la gestione dell'emergenza: il comitato di crisi

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

Le figure minime necessarie per la costituzione del Comitato di Crisi sono rappresentate da:

- un ruolo di vertice con poteri decisionali e di indirizzo in materia organizzativa ed economica, ovvero il responsabile dell'Ufficio Unico Dirigenziale ex art. 17 del CAD;
- il responsabile della "continuità operativa" dell'ente;
- il responsabile dell'Unità locale di sicurezza prevista dal DPCM 01.04.2008 (se presente);
- il responsabile dell'informatica dell'ente (se previsto dall'organizzazione dell'ente);
- il responsabile della sicurezza dell'ente, come previsto dalla 81/2008.

In condizioni ordinarie il Comitato si riunisce con periodicità almeno annuale, allo scopo di valutare lo stato della soluzione di continuità ICT, verificare le criticità, attuare e pianificare le iniziative per il miglioramento continuo dei processi che garantiscono la continuità operativa.
I principali compiti del Comitato di Crisi in condizioni ordinarie sono:

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

In condizioni di emergenza ICT, il Comitato assume il controllo di tutte le operazioni e assume le responsabilità sulle decisioni per affrontare l'emergenza ICT, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.
I principali compiti del Comitato di Crisi, in condizioni di emergenza ICT sono:

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

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

- comunicazioni, ad esempio tramite valutazione delle strategie di comunicazione verso cittadini, organizzazioni e dipendenti e dei canali da utilizzare per ciascun tipo di comunicato;
- finanza, ad esempio con definizione di tutte le iniziative di carattere finanziario necessarie ad assicurare risorse tempestive;
- risorse umane e rapporti sindacali, ad esempio per la definizione di comportamenti e la formulazione di messaggi specifici volti a rassicurare i dipendenti, sensibilizzare quelli coinvolti nelle operazioni di ripristino, dirimere ogni possibile motivo di disagio che possa ridurre l'efficacia dell'organizzazione;
- sicurezza informatica, con l'esame di tutti gli aspetti di sicurezza, in particolare per quanto riguarda la verifica del grado di sicurezza offerto dalle configurazioni adottate per l'emergenza ICT e la protezione dei dati, o tramite il riesame delle soluzioni adottate per il ripristino dei sistemi e per il ritorno alla normalità;
- area legale, per eventuali azioni nei confronti del fornitore della soluzione di Continuità Operativa (es. per il mancato rispetto dei tempi di RTO/RPO).

Si rammenta, comunque, la necessità per le Amministrazioni di rispettare, nella complessiva definizione della politica di Continuità Operativa dell'ente, gli adempimenti imposti dal quadro

normativo vigente in materia di protezione dei dati personali (D. Lgs. 196/2003) chiarendo in modo esplicito i soggetti che effettuano il trattamento, con particolare riferimento al responsabile e agli incaricati del trattamento, tenuto conto di quanto previsto dagli art. 29 e 30 del richiamato Codice in materia di protezione dei dati personali.
L'Amministrazione dovrà, infatti, assicurare la piena conformità agli obblighi previsti dalla normativa del Codice in materia di protezione dei dati personali e dai provvedimenti del Garante per la protezione dei dati personali, con particolare riferimento alle misure di sicurezza e all'individuazione delle figure dei responsabili, degli incaricati al trattamento e degli Amministratori di sistema, prevedendo anche le necessarie attività di verifica e controllo. Al proposito, si ricorda anche l'importanza di osservare i provvedimenti fra cui il provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministrazione di sistema" del 27 novembre 2008.

4 LA REALIZZAZIONE DELLA CONTINUITÀ OPERATIVA E DELLE SOLUZIONI DI DISASTER RECOVERY

Nel presente capitolo vengono fornite indicazioni sul percorso e gli strumenti da utilizzare per individuare i Tier e poi impostare il progetto e definire tempestivamente i PCO e PDR che consentiranno alle Amministrazioni di dotarsi di soluzioni di continuità operativa dei servizi in linea con il proprio contesto tecnico operativo di riferimento, prevedere gli opportuni meccanismi di verifica periodica e di manutenzione nel tempo indispensabili a rendere la soluzione individuata adeguata anche a fronte di rilevanti variazioni tecnico organizzative.

4.1 Determinazione delle esigenze di continuità e delle soluzioni

Ferma restando la necessità per le Amministrazioni di assicurare la Continuità dei servizi critici, tenuto conto degli aspetti delineati nei precedenti capitoli, di regola non è possibile individuare la soluzione di CO e di DR più opportuna senza una preventiva analisi delle conseguenze dei possibili scenari determinati da eventi negativi che determinino un fermo dichiarato delle funzionalità dell'infrastruttura informatica.

Si tratta di svolgere una "analisi di impatto", che prevede anche la valutazione dei rischi (si veda al riguardo l'appendice al presente documento) per condurre ad una stima da parte dell'Amministrazione delle tolleranze socialmente accettabili nei confronti dell'interruzione di un canale comunicativo (verso i cittadini, verso le imprese, verso altre Amministrazioni, verso la propria utenza interna).
Attesa, pertanto, la necessità di definire attraverso queste Linee Guida le modalità secondo le quali le amministrazioni dovranno procedere alla redazione degli studi di fattibilità per la continuità operativa da sottoporre all'Agenzia, come previsto dal CAD, è stato definito un percorso di autovalutazione cui i singoli enti potranno sottoporsi per l'identificazione delle possibili soluzioni tecnologiche rispondenti alle peculiari caratteristiche e specificità, identificate in base alla:

- tipologia di servizio erogato;
- complessità organizzativa;
- complessità tecnologica.

Concettualmente l'attività di autovalutazione procede lungo un percorso metodologico tramite il quale ciascuna Amministrazione, applicando un semplice strumento di supporto guidato, procede ad un'analisi quali-quantitativa delle criticità il cui risultato le consente di collocarsi all'interno di una specifica classe di rischio/criticità tra quelle previste. A ciascuna di esse, definite secondo caratteristiche omogenee, corrisponde una determinata classe di soluzioni. Le indicazioni risultanti potranno essere utilizzate per la redazione di uno Studio di Fattibilità Tecnica idoneo alle esigenze del profilo stesso, che l'Amministrazione potrà utilizzare come strumento sul quale basare il percorso per la richiesta di parere tecnico all'Agenzia per l'Italia.

L'analisi proposta si fonda, come elemento di riferimento, sulla logica del servizio erogato dalla singola Amministrazione, in un'ottica secondo cui la criticità delle attività svolte (e quindi le esigenze in termini di RTO/RPO) non può essere semplicemente inferita in termini direttamente proporzionali alla dimensione dell'Amministrazione stessa ma deve essere valutata portando in conto anche altri parametri di riferimento, tra cui principalmente la natura e tipologia dei servizi erogati ed il danno/impatto atteso sugli utilizzatori in caso di sospensione del servizio stesso.

L'Amministrazione deve tener conto, nell'attuazione del percorso delineato per l'attuazione delle soluzioni di continuità operativa e Disaster Recovery:

- delle regole del rispettivo comparto di appartenenza per garantire la permanenza nel tempo della fruibilità dei dati;
- delle prescrizioni del D.lgs. n. 196/2003 (contenente le disposizioni del "Codice in materia di Protezione dei dati personali") e s.m.i. e dei provvedimenti del Garante;
- delle regole tecniche che sono in corso di emanazione per la corretta gestione documentale, in linea con i principi del C.A.D;
- della necessità di implementare e attuare corrette politiche di backup dei dati, degli archivi e dei log.

Ai fini di quanto previsto dall'art. 50-bis comma 4, al termine del percorso di autovalutazione si può quindi individuare, nelle soluzioni proposte, quella più aderente all'Amministrazione.

Come si è già avuto modo di accennare nel precedente capitolo 2, non è escluso che l'attuazione della norma citata, lo svolgimento del percorso proposto, l'analisi e la verifica periodica dell'adeguatezza e del costante aggiornamento della soluzione, possano comportare, come del resto è nello spirito del CAD, una verifica e revisione del modo di operare delle Amministrazioni e del Sistema Primario (da punto di vista infrastrutturale e applicativo) sulla base del quale è stata scelta la soluzione di CO, stimolando le Amministrazioni stesse ad una maggiore razionalizzazione e digitalizzazione dei servizi ICT.

In particolare tale adempimento è da ritenersi inderogabile per la corretta gestione del sistema di conservazione.

Il percorso di autovalutazione e lo schema di Studio di Fattibilità Tecnica, descritti più in dettaglio nel seguito, dovranno essere adottati da tutte le Amministrazioni sia che abbiano già adottato soluzioni e piani di CO/DR – come strumento per sottoporre al parere di DigitPA la soluzione in essere e verificarne l'aderenza alle linee guida – sia che debbano adottare ex novo lo studio di fattibilità tecnica e sulla base dello stesso i piani di CO/DR.

Le tabelle e gli esiti del percorso di autovalutazione saranno inviati all'Agenzia, in formato elettronico, in allegato allo Studio di Fattibilità Tecnica.

4.2 Cenni alle modalità per condurre un analisi di impatto nella determinazione delle esigenze di continuità

L'analisi di impatto (BIA) identifica le funzioni critiche per il business, stabilisce le priorità tra le funzioni e determina l'impatto sull'organizzazione se queste funzioni non sono effettuate in un periodo di tempo specificato, secondo i passaggi di massima di seguito schematicamente suggeriti:

1. analizzare i worst-case scenarios
    a. la perdita di un sito a causa di un problema elettrico o incendio;
    b. l'impossibilità ad accedere agli edifici;
    c. l'inabilità degli impiegati a lavorare;
    d. il guasto ai sistemi informativi;
    e. problemi a terze parti che impattano i servizi essenziali;
    f. incidenti derivanti dall'ambiente;
2. identificare i servizi essenziali in termini di attività e responsabilità;

3. condurre le interviste per raggiungere i seguenti 4 obiettivi:
    a. quali processi sono mission-critical;
    b. quale è l'RTO;
    c. quel è l'RPO;
    d. qual è l'impatto dell'interruzione e del relativo downtime?
    e. chiedendo:
        – Qual è l'effetto di un incidente che dura 1 ora, 1 giorno, 1 settimana…?
        – Quanto velocemente si deve ridare servizio?
        – Quanti dati si possono perdere tra il momento dell'incidente e quando si ripristina il servizio?
        – Qual è il numero minimo di persone per ruolo che sono necessarie per supportare il recovery?
        – Quali procedure di contingency esistono?
        – Quali applicazioni supportano il tuo processo?
        – Quali dipendenze con terze parti?
4. fare una normalizzazione della valutazione dell'impatto;
5. "prioritizzare" i servizi critici.

4.3 Strumenti per l'autovalutazione

La redazione dello Studio di Fattibilità Tecnica è il momento finale di un *percorso metodologico* che l'Amministrazione deve effettuare.

Al fine di perseguire l'obiettivo di omogeneità di soluzioni che si prefigge il CAD, e soprattutto, senza voler prescindere dai percorsi e dalle metodologie esistenti, con particolare riguardo alla BIA e alla RA, al fine di coadiuvare le Amministrazioni ad ottemperare, nei tempi previsti agli obblighi previsti dall'art. 50-bis del CAD, si è ipotizzato, come già detto, un percorso guidato che, a seguito di una fase di autovalutazione semplificata svolta dall'Amministrazione, la faccia ricadere in una delle classi prestabilite in cui sono raggruppate le possibili tipologie omogenee di soluzioni.

Tale autovalutazione, che si basa su tre direttrici di analisi, permette di avere un quadro di sintesi delle esigenze dell'Amministrazione, che possono essere raggruppate in classi. L'appartenenza ad una classe determina la possibilità di restringere ad una tipologia le soluzioni al fine soddisfare le esigenze.

Oltre alle soluzioni, la classe di appartenenza è di supporto a restringere il campo dei requisiti tecnico/organizzativi che dovrebbero essere soddisfatti e che andranno riportati nello studio di fattibilità, così come la soluzione scelta. Nella redazione dello studio si dovrà utilizzare il *template* riportato nel presente documento al capitolo 5.

E' rimessa alle decisioni dell'amministrazione la valutazione dell'adozione della soluzione prevista per i servizi ICT più critici ovvero la scelta di diversificare in base alla classe di rischio individuata per i differenti servizi censiti.

4.2.1 Le direttrici di analisi

La stima sulla criticità dei servizi viene supportata nello strumento adottato dalla valutazione pesata di alcuni semplici indicatori appartenenti alle seguenti tre *direttrici*, le quali si riferiscono all'attività e alla strutturazione organizzativa dell'Amministrazione, oggetto di analisi:

- direttrice del **servizio**;
- direttrice dell'**organizzazione**;
- direttrice della **tecnologia**.

Tali direttrici, ed i relativi indicatori, sono state scelte in quanto ritenute l'insieme in grado di descrivere al meglio gli aspetti di complessità di un'Amministrazione e di criticità dei servizi da essa erogati, pur mantenendo ad un livello di accettabile semplificazione l'analisi e la valutazione sottostante.

In particolare:

- la direttrice del *servizio* consente di far rientrare nella valutazione aspetti legati alla tipologia, numerosità e criticità dei servizi erogati, in termini di danno per l'organizzazione e/o per i suoi utenti in caso di mancata erogazione del servizio stesso;
- la direttrice dell'*organizzazione* consente di far rientrare nella valutazione aspetti legati alla complessità amministrativa e strutturale dell'organizzazione, al fine di stimare il dimensionamento delle soluzioni tecnologiche da adottare;
- la direttrice della *tecnologia* consente di far entrare nella valutazione aspetti legati al fattore tecnologico in termini di dimensione e complessità, al fine di poter stimare la tipologia e la natura delle soluzioni tecnologiche da adottare.

4.2.2 I criteri di stima

Per poter procedere alla definizione di un valore che possa aiutare una Amministrazione a valutare in forma sintetica il livello di tolleranza dei propri servizi nei confronti della loro eventuale indisponibilità sono stati individuati specifici indicatori lungo ciascuna delle tre direttrici sopra indicate. Ai criteri generali individuati per ciascuna direttrice, e riassunti qui di seguito, sono stati associati uno o più parametri di dettaglio il cui elenco analitico è riportato nel prosieguo.

Con riguardo alla direttrice del *servizio* i criteri identificati sono:

- tipologia di utenza;
- tipo di dati trattati;
- l'interruzione blocca un processo;
- modalità prevalente di interazione con gli utenti;
- giorni alla settimana nei quali viene erogato il servizio;
- ore al giorno nelle quali viene erogato il servizio;
- sono presenti procedure alternative;
- è possibile recuperare la mancata acquisizione dei dati;
- è necessario recuperare i dati non acquisiti;
- l'interruzione determina un immediato disagio agli utenti;
- principale danno per l'Amministrazione;
- livello di danno per l'Amministrazione;
- principale tipo di danno per l'utente finale;
- livello di danno per l'utente finale;

- tempo massimo tollerabile tra la produzione di un dato e il suo salvataggio;
- tempo di indisponibilità massima del servizio.

Con riguardo alla direttrice della *organizzazione* i criteri identificati sono:
- numero di Unità Organizzative;
- numero di sedi;
- dimensione territoriale;
- numero dei responsabili del trattamento dei dati;
- numero dei trattamenti censiti;
- numerosità degli addetti tramite i quali vengono erogati i servizi;
- numerosità degli utenti esterni.

Con riguardo alla direttrice della *tecnologia* i criteri identificati sono:
- presenza di un dipartimento IT;
- numerosità addetti IT;
- architettura elaborativa;
- architettura applicativa;
- numero di server;
- numero di postazioni di lavoro;
- numero degli archivi utilizzati dal servizio;
- dimensione totale degli archivi usati dal servizio;
- istanze di DB usate dal servizio.

Sulla base di tali criteri è possibile individuare un indicatore di sintesi (Indicatore complessivo di criticità), che identifica il livello di criticità dei servizi. I suddetti livelli di criticità vengono raggruppati in 4 Classi: Bassa, Media, Alta e Critica.

4.2.3 Le tipologie di soluzioni tecniche

Uno degli obiettivi che si prefigge il Codice dell'Amministrazione Digitale è quello di giungere ad un'omogeneizzazione delle soluzioni di continuità operativa e Disaster Recovery.

A tal fine si è proceduto ad individuare delle soluzioni, indicate convenzionalmente come Tier 1, Tier 2, …, Tier 6; ciascuna classe di criticità dovrebbe condurre all'individuazione almeno dei Tier che, come ipotizzato nello schema di seguito riportato, si ritiene siano quelli più adatti; resta ferma la discrezionalità dell'Amministrazione di decidere eventualmente soluzioni, modalità di backup e ripristino più elevate di quelle minimali individuate per la classe di criticità ed indicate in via esemplificativa nella tabella seguente (non escludendo quindi ad es. la possibilità di adottare, per servizi con classe di criticità bassa o media, modalità di backup e soluzioni tipiche di una classe di criticità più elevata; ovvero non eliminando, la possibilità, per casi riconducibili a soluzioni Tier 1 e 2, di adottare modalità di back up "via rete").

Possono, infatti, coesistere diverse soluzioni, la scelta delle quali dipende da ulteriori fattori legati al contesto organizzativo e/o tecnologico nonché finanziario di riferimento. Ove ad esempio il profilo finanziario comporti un ostacolo all'adozione della soluzione più adeguata alla classe di rischio individuata al termine del percorso, imponendo ad es. la scelta di una soluzione Tier 4 per una classe "critica", l'Amministrazione, come si avrà modo di evidenziare più diffusamente nel successivo capitolo, dedicato alle indicazioni da inserire nello studio di fattibilità, dovrà dare evidenza delle

motivazioni e dei vincoli che determinano la scelta adottata e dei tempi stimati per realizzare, invece, le soluzioni che sarebbero più confacenti alla classe di rischio individuata.

È necessario, comunque, sottolineare che, indipendentemente dal tipo di soluzione che la singola amministrazione intende adottare, essa deve sempre assicurare la conformità con quanto previsto dal D. Lgs. 196/03 e s.m.i. ("Codice in materia di protezione dei dati personali") e dai connessi provvedimenti del Garante, relativamente alle misure tecniche ed organizzative da adottare per la protezione dei dati personali trattati dall'Amministrazione.

Le tipologie di soluzioni tecniche elencate qui di seguito sono definite in senso generale con riguardo alle funzionalità richieste e/o da assicurare e come tali non fanno riferimento a specifiche tecnologie e/o prodotti o soluzioni di mercato.

***Tier 1**:* è la soluzione minimale coerente con quanto previsto dall'articolo 50-bis. Prevede il backup dei dati presso un altro sito tramite trasporto di supporto (nastro o altro dispositivo). I dati sono conservati presso il sito remoto. In tale sito deve essere prevista la disponibilità, in caso di emergenza, sia dello storage disco dove riversare i dati conservati, sia di un sistema elaborativo in grado di permettere il ripristino delle funzionalità IT. Nel caso di affidamento del servizio di custodia ad un fornitore, tale disponibilità deve essere regolamentata contrattualmente.
Per questa soluzione:

- potrebbero non essere presenti procedure di verifica della presenza dei dati sul supporto, della coerenza dei dati ed esistere un'unica copia storage;
- la disponibilità dei dispositivi (storage disco e sistemi di elaborazione) potrebbe prevedere tempi non brevi (anche più settimane per l'assegnazione da parte del fornitore);
- la disponibilità dei dispositivi potrebbe non garantire le performance rispetto al sistema primario;
- la disponibilità dei dispositivi potrebbe essere assegnata per un periodo di tempo limitato.

Poiché i dati salvati possono essere relativi all'intera immagine dello storage primario o solo ai dati delle elaborazioni, la disponibilità dei dispositivi ausiliari deve essere chiaramente definita in termini di ambiente hardware e software di riferimento.
Vengono quindi assicurate l'esecuzione e conservazione dei backup e, per i casi in cui si renda necessario assicurare il ripristino, la disponibilità di un sito "vuoto" attrezzato, pronto a ricevere le componenti e configurazioni necessarie, ove fosse richiesto, per far fronte all'emergenza (*on demand*).

***Tier 2**:* la soluzione è simile a quella del Tier 1, con la differenza che le risorse elaborative possono essere disponibili in tempi sensibilmente più brevi, viene garantito anche l'allineamento delle performance rispetto ai sistemi primari ed esiste la possibilità di prorogare, per un tempo limitato, la disponibilità delle risorse elaborative oltre il massimo periodo di base.
Vengono assicurate l'esecuzione e conservazione dei backup e la disponibilità presso il sito dei sistemi e delle configurazioni da poter utilizzare per i casi in cui si renda necessario il ripristino.

***Tier 3**:* la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare).Va periodicamente verificato l'allineamento dei dati.

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

Tier 5*:* la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti (aggiornamento sincrono). Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario. Debbono essere attentamente valutati se sussistono, per aspetti tecnologici, vincoli di operatività del sito primario in caso di problemi su quello secondario. E' quindi fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.

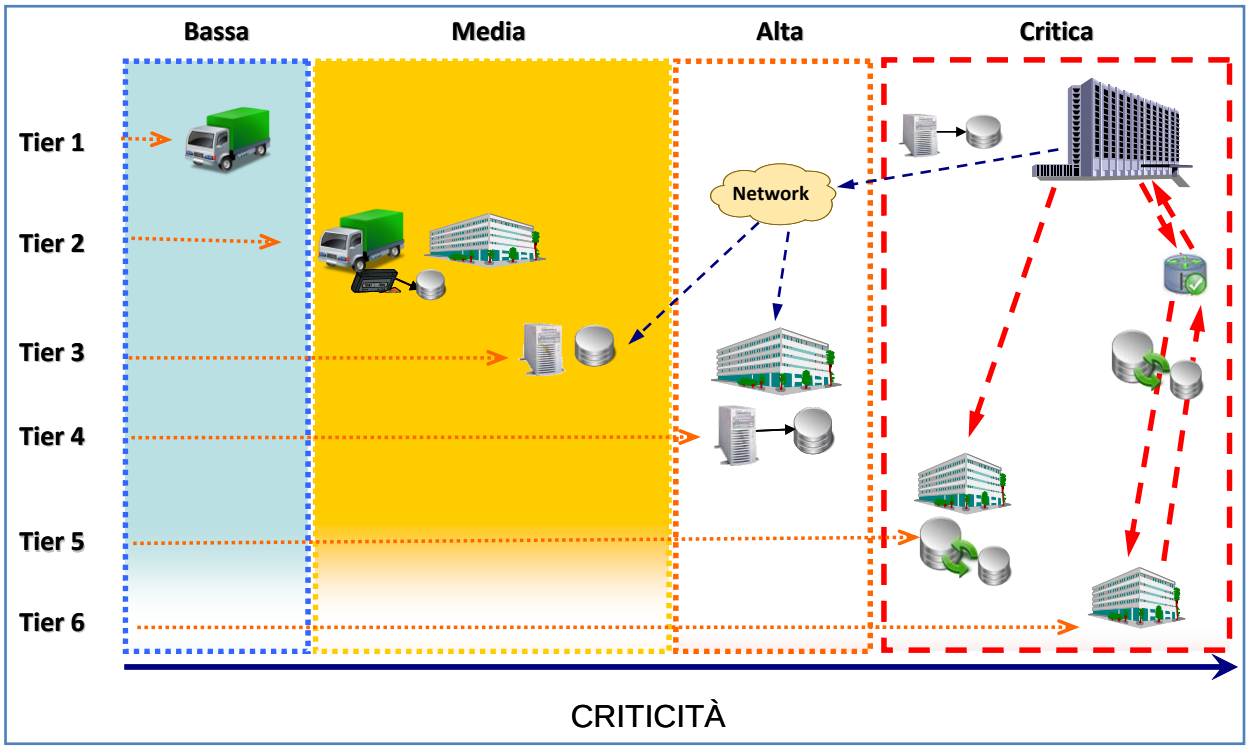
Tier 6*:* la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività dell'IT in tempi molto ristretti. Le altre caratteristiche sono uguali a quelle del Tier 5.
E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.

Anche alla luce dell'esperienza maturata nell'analisi delle richieste di parere, a puro titolo indicativo (e non vincolante), si possono riepilogare come segue, gli elementi di massima dei Tier delineati e precedentemente descritti:

I LIVELLI DELLE SOLUZIONI ***(Tier LG)***	**PRINCIPALI INDICATORI**			**ELEMENTI DI MASSIMA DELLA SOLUZIONE TECNICA (SOLUZIONI ALMENO A 2 SITI)**	
	RTO		**RPO max**	***Modalità minime di copia/aggiornamento per il conseguimento dei valori max di RPO***	***Aspetti minimali connessi al sito di DR***
	Min	Max			
Tier 1*:*	7g	>7 gg solari	max 7gg solari	Copia su supporti rimuovibili	Sito esistente ma da attrezzare con risorse elaborative/ server solo reperibili. Il sito di DR è predisposto ad accogliere personale e apparecchiature, ma rimane privo di risorse fino al momento di effettiva necessità. Di solito consiste solo di un ambiente fisico dotato di corrente elettrica e di rete dati con idonee misure di sicurezza (es: sistema antincendio ed antifumo; sistema antiallagamento; sistema di alimentazione in grado di garantire l'erogazione di energia elettrica anche a fronte di prolungate interruzioni di alimentazione nella cabina di fornitura; sistema d'aria condizionata per garantire temperatura ed umidità costante; impianto per il ricambio d'aria; sistema di accesso controllato).
Tier 2: .	3g	max 7 gg	max 7 gg solari	Copia su supporti rimuovibili	Il sito dispone di hw e connettività già funzionante ma su scala inferiore rispetto al sito principale o a un sito alternativo sempre disponibile e con replica costante dei dati.
Tier 3:	1g	3g	Max 1 gg	Electonic vaulting: soluzione che comporta il backup dei dati presso il sito alternativo in maniera elettronica, con una riduzione del tempo necessario per il trasporto dei dati e la possibilità di un recovery time piu' veloce.	Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un site alternativo sempre disponibile e con replica costante dei dati. Il backup avviene in modalità elettronica e quindi sono necessari collegamenti fra i siti tenuto conto della tipologia, quantità e periodicità dei dati da backup-are

I LIVELLI DELLE SOLUZIONI *(Tier LG)*	PRINCIPALI INDICATORI			ELEMENTI DI MASSIMA DELLA SOLUZIONE TECNICA (SOLUZIONI ALMENO A 2 SITI)	
	RTO		RPO max	*Modalità minime di copia/aggiornamento per il conseguimento dei valori max di RPO*	*Aspetti minimali connessi al sito di DR*
	Min	Max			
Tier 4:	4h	3gg	Max 4 h	Asincrono On line (risorsa storage accesa)	Il sito alternative è solitamente "un duplicato" del sito originale con tutti i sistemi hardware e la quasi totalità dei backup di dati disponibile. Il sito alternativo può essere pronto ed operativo in alcune ore o meno. Nel caso in cui il personale deve essere spostato fisicamente presso il sito secondario, il sito risulterà operativo solo dal punto di vista del data processing. La piena operatività sarà raggiunta quando anche il personale avrà raggiunto il sito.
Tier 5:	1h	max 4 h	max 5 min	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi ciascuno con capacità sufficiente a prendere in carico il lavoro dell'altro e in cui l'aggiornamento del dato avviene solo quando entrambi i siti hanno completato l'update (con perdita dei soli i dati che in quel momento stanno per essere processati). E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.
Tier 6:	0m	1h	Zero min.	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi, ognuno dei quali possiede capacità sufficienti a farsi carico del lavoro dell'altro; in questa soluzione il carico di lavoro da un sito all'altro si trasferisce immediatamente ed automaticamente. E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.

La figura che segue riassume quanto sopra esposto, ed esemplifica i Tier di massima (per soluzioni ad almeno due siti alternativi):



4.4 Ulteriori elementi che possono essere tenuti presenti

Nell'individuazione della soluzione che si intende adottare è opportuno individuare la strategia di salvataggio dei dati ad esempio: locale/remoto; *on-line/off-line*; il tipo di trasferimento e la periodicità; il tipo di salvataggio (totale/incrementale); le modalità di conservazione.
E' importante anche decidere se la soluzione salvaguarda allo stesso modo tutti gli applicativi che permettono l'abilitazione del servizio o gruppi di servizi e prevedere un'eventuale mappa di copertura che indichi per il singolo servizio il livello di copertura (parziale o totale), nonché decidere se e come la soluzione copre i server che ospitano gli applicativi, oppure se sia prevista una copertura parziale.
Ove si intenda dotarsi di un sito secondario, è necessario considerare:

- le caratteristiche dei collegamenti tra il sito primario ed il secondario, in termini di capacità di trasmissione, di disponibilità, di ridondanza e possibilità di collegamenti alternativi, ponendo attenzione in merito a come tali caratteristiche permettano di soddisfare in maniera totale o parziale le esigenze del servizio;
- le modalità di recupero dei dati e di verifica della loro consistenza e completezza;
- se e come il servizio erogato dal sito secondario abbia le stesse caratteristiche di quello primario;
- le modalità di test del disaster recovery.

4.3.1 Cenni sulle modalità di realizzazione delle soluzioni

Dal punto di vista realizzativo, rimandando per quanto attiene alle modalità di realizzazione e agli strumenti giuridici ed operativi attuabili al successivo capitolo 6, va, comunque, sottolineato che, nell'ottica dell'art. 50-bis del CAD, un servizio di DR non può considerarsi tale se non prevede una locazione alternativa a quella dove vengono gestite le elaborazioni e conservati i dati delle stesse. Inoltre, tutte le soluzioni non richiedono teoricamente che queste vengano attuate ricorrendo in ogni caso a fornitori esterni: un'Amministrazione potrebbe decidere di realizzare la soluzione utilizzando locali, infrastrutture e personale proprio.
Laddove è possibile, come si avrà modo di evidenziare sempre nel successivo capitolo 6, può essere opportuno verificare la possibilità che, indipendentemente dalla soluzione adottata e dalla realizzazione di questa (tramite strutture proprie o fornitori di servizio esterni) più Amministrazioni concorrano alla realizzazione della soluzione stessa, utilizzando le forme associative richiamate in queste linee guida.

4.3.2 Cenni su aspetti tecnologici che possono orientare la scelta delle soluzioni

Soluzioni tecnologiche basate su virtualizzazione e ancor di più su architetture cloud non sono esenti dalla necessità di valutare tutti gli aspetti di sicurezza, a garanzia di disponibilità, integrità e confidenzialità dei dati. A tal fine, a seconda delle specifiche esigenze e del contesto di riferimento, è rimessa alla prudente valutazione dell'Amministrazione l'adozione delle soluzioni di seguito accennate come modalità per realizzare soluzioni di CO e di DR.

4.3.2.1 La virtualizzazione

Con il termine "*virtualizzazione*" si intende la completa emulazione in software di un ambiente fisico e logico di calcolo. Ad esempio su una singola risorsa hardware la virtualizzazione permette l'esecuzione contemporanea di più sistemi operativi, completamente svincolati tra di loro.
La virtualizzazione permette anche, in fase di upgrade/sostituzione di un server; di riconfigurare da zero il sistema operativo e le applicazioni necessarie.

Inoltre la virtualizzazione consente di ridurre i costi in quanto, pur utilizzando server con caratteristiche più elevate, è possibile ridurne il numero e di conseguenza i costi di manutenzione.
Benefici in termini di riduzione dei costi possono essere conseguiti anche adottando tecniche di virtualizzazione dei client nel caso in cui le postazioni di lavoro della soluzione di CO e di DR siano sottoutilizzate o spente, potendo quindi essere richieste *on demand.*
Le stesse considerazioni valgono ovviamente anche per il sito primario, anzi un'architettura del genere permette di avere ulteriori vantaggi per le procedure di salvataggio e di Disaster Recovery in quanto è possibile effettuare copia delle immagini delle risorse virtualizzate consentendo ripristini in tempi brevi.

Nel caso in cui nel sito secondario sia presente una architettura virtualizzata è necessario avere chiaro se e come avviene il *mapping* tra server virtuale del sito secondario e server fisico o virtuale del primario, indicando eventualmente i server o gli applicativi che non sono coperti dalla soluzione e le eventuali ricadute sul servizio.
Se sia il sito primario, sia il sito secondario adottino una architettura virtualizzata, è necessario indicare se esiste corrispondenza tra i server fisici.
Si sottolinea il fatto che non tutte le applicazioni sono virtualizzabili e pertanto va verificato se procedere in tal senso.

4.3.2.2 Le soluzioni cloud

Con il termine "*cloud computing"* si intende la disponibilità, in modalità "*on demand"*, di risorse informatiche (applicazioni, DB, file service…) viste come *servizi* tramite l'accesso ad una rete di computer la cui reale dislocazione sul territorio può essere sconosciuta all'utente, il quale, quindi, può operare ignorando la reale natura, struttura e collocazione delle risorse impiegate, utilizzandole in modalità *"service"* e accedendo o tramite Internet (*Public cloud*) o tramite intranet private (*Private cloud*).

Nel caso del modello *"public cloud"* i servizi sono offerti da fornitori che mettono a disposizione dei propri utenti/clienti la potenza di calcolo e/o di memorizzazione dei loro data center.
Il cloud privato viene installato dall'utente nel suo data center per suo utilizzo esclusivo.
I due modelli di cloud (*private, public*) possono coesistere in quello che viene definito *Hybrid cloud*.

Il *cloud computing* può offrire un'alternativa interessante ai modelli tradizionali di disaster recovery. Dall'esame degli studi di fattibilità pervenuti da amministrazioni locali di dimensioni medio-piccole si riscontra un interesse crescente verso soluzioni di DR basate su servizi cloud. Contemporaneamente si rileva sul mercato, anche nel nostro paese, una crescita del numero di operatori che offrono questi servizi che rientrano nel modello di servizio definito *"Infrastructure as a service"* (IaaS).

Tale modello prevede l'offerta di una infrastruttura con capacità computazionale, di memorizzazione e di rete sulla quale l'utente può installare ed eseguire il software necessario, dal sistema operativo alle applicazioni.
Nel caso di servizio computazionale, l'utente può richiedere al fornitore di servizi un insieme di macchine virtuali, sulle quali può installare i sistemi operativi ed i software adatti alle proprie esigenze. Le macchine virtuali sono raggiungibili per la loro gestione ed utilizzo tramite l'interfaccia offerta dal fornitore del servizio. Una volta che le macchine virtuali sono state assegnate all'utente, egli può richiederne delle nuove o rilasciarne alcune, in base alle sue esigenze.
Nel caso di servizio di memorizzazione, invece, l'utente può richiedere uno spazio di memorizzazione per caricarvi i suoi dati e, successivamente, può aumentarlo o ridurlo a seconda delle sue esigenze.

I servizi *cloud* di DR si basano su infrastrutture virtualizzate e quindi sono particolarmente adatti a fornire soluzioni di DR a utenti con infrastrutture virtualizzate nel sito primario. E' sufficiente assicurarsi che gli strati di virtualizzazione siano compatibili.
E' possibile l'utilizzo di servizi cloud anche nel caso di presenza di sistemi fisici nel sito di produzione, procedendo alla conversione *phisical-to-virtual* al momento del trasferimento nel *cloud* o al momento della attivazione delle macchine virtuali nella infrastruttura cloud.

I servizi *cloud* per il DR rientrano in due categorie principali:

- servizi cloud di DR costruiti dall'utente combinando servizi IaaS;
- servizi cloud definiti *"DR as a service*" (DRaaS).

Nel primo caso l'utente realizza una soluzione di DR su misura per le proprie esigenze combinando in modo adeguato servizi IaaS di storage e di risorse elaborative offerte dal fornitore di public cloud, gestendo in proprio il trasferimento dei dati e delle immagini delle macchine virtuali nel cloud, il ripristino in caso di disastro e l'eventuale conversione a server virtuali di server fisici presenti nel sito primario. La amministrazione utente del servizio deve avere personale competente in quanto, per queste soluzioni "fai da te", il fornitore, generalmente, non fornisce servizi di supporto per il trasferimento dati e immagini nel cloud, per il ripristino e per la eventuale conversione *phisical-to virtual*.

Nel secondo caso si tratta di servizi preconfezionati definiti "*DR as a service*" finalizzati a consentire, in caso di disastro, il ripristino dei sistemi di produzione dell'utente nella infrastruttura cloud con requisiti di RPO e RTO predefiniti in funzione del livello di servizio prescelto. Spesso i fornitori di servizi DRaaS forniscono software per replicare i dati e le applicazioni presenti nel sito primario dell'utente al cloud e sono in grado di convertire back-up di macchine fisiche o virtuali in macchine virtuali da attivare nel cloud.

Nel caso dei servizi cloud del tipo DRaaS i fornitori prevedono generalmente livelli di servizio diversi in relazione alle esigenze dell'utente, con costi crescenti al decrescere dei valori previsti di RTO e RPO. I livelli tipici rilevati dagli analisti di mercato internazionali sono i seguenti:

***Hot cloud site*:** per garantire tempi di RTO/RPO prossimo allo zero le macchine virtuali sono sempre attive nel cloud con replica in tempo reale delle macchine virtuali tra sito di produzione e infrastruttura cloud.
(RTO: 0-2 ore, RPO: 0-24 ore)

***Warm cloud site*:** nel cloud sono presenti copie non in linea delle macchine virtuali che possono essere attivate in caso di disastro o per attività di test con tempi di ripristino di poche ore
(RTO: 2-6 ore, RPO: 0-24 ore)

***Cold cloud site*:** nel cloud sono conservati i backup dei sistemi di produzione che possono essere convertiti in macchine virtuali prima del ripristino al momento del disastro; è anche possibile che l'utente trasferisca nella infrastruttura cloud al momento del disastro e del ripristino le immagini e i dati conservati su nastro o disco in altri siti.
(RTO: 4-24 hours, RPO: 24-48 hours)

Si ritiene che il livello "*warm cloud site*" sia in grado di rispondere alle esigenze di DR delle piccole e medie amministrazioni per la maggior parte dei servizi erogati.

E' comunque possibile adottare soluzioni a più livelli in funzione della diverse criticità dei servizi. Qualora più macchine virtuali supportino la stessa applicazione o servizio erogato è necessario che vengano assegnate allo stesso livello di servizio al fine di garantire la consistenza e la sincronizzazione nelle operazioni di ripristino e di rientro nel sito primario.

Il principale vantaggio dei servizi di DR basati sul *cloud* è quello di presentare tempi di ripristino simili a quelli delle soluzioni di DR basate su risorse dedicate con costi prossimi a quelli delle soluzioni basate su risorse condivise.
Il *cloud* è intrinsecamente un'infrastruttura condivisa: un insieme di risorse, con costi infrastrutturali distribuiti tra tutti coloro che stipulano contratti per utilizzare queste risorse come servizio. La maggior parte del tempo si pagano essenzialmente solo le risorse di archiviazione, mentre le macchine virtuali vengono attivate solo in caso di emergenza o di test, ad eccezione delle soluzioni *hot cloud site*.
I tempi di ripristino delle macchine virtuali sono contenuti, anche nel caso di macchine virtuali fuori linea, mentre i costi sono quelli delle strutture condivise.

Altri vantaggi sono i seguenti:
- la natura flessibile dei contratti *cloud* basati sull'utilizzo *on demand* di risorse pagate in base all'uso comporta che l'investimento iniziale è nullo o molto basso e che sia facile adattarsi ai cambiamenti dell'ambiente IT e alle esigenze dell'utente;
- i tempi per l'avvio della soluzione di DR sono ridotti (settimane, non mesi o anni) in quanto la soluzione è semplice e veloce da realizzare, dal momento che gran parte delle operazioni di configurazione possono essere effettuate online, e che non è necessario allocare hardware identico a quello del proprio sistema IT, impostare connessioni proprietarie o negoziare livelli di servizio specifici;
- le attività di test sono più facili e meno costose e possono essere più frequenti; le procedure di test possono essere automatizzate e svolte senza interruzioni; i contratti DRaaS di solito includono servizi di test e la assistenza per il ripristino.

I servizi cloud vengono di solito fruiti attraverso una connessione Internet e pertanto la Amministrazione deve valutare se il servizio di connettività fornito dall'ISP sia adeguato in relazione ai requisiti definiti nello studio di fattibilità e nel successivo piano di continuità ICT.

Come per tutti i servizi in outsourcing occorre verificare che il sito o i siti dove viene erogato il servizio abbia/no almeno i requisiti minimi riportati nell'allegato della scheda D3 del documento *"I SERVIZI MINIMI ESSENZIALI PER L'ADOZIONE DELLE SOLUZIONI DI DISASTER RECOVERY, IN LINEA CON L'ART. 50-BIS DEL CAD*" pubblicato nel sito dell'Agenzia.
Occorre altresì verificare la presenza dei processi gestionali descritti al punto 3.3 delle presenti linee guida.

Ci sono inoltre aspetti specifici connessi alla natura particolare dei servizi cloud che la Amministrazione utente deve tenere in considerazione:
- natura intrinsecamente multi utente dei servizi *"public cloud"*
- possibile localizzazione della infrastruttura geograficamente distribuita.

Per l'approfondimento di questi aspetti si rimanda al capitolo 6.

4.3.2.3 La connettività e gli aspetti di sicurezza della rete

Fermo restando l'obbligo per le pubbliche amministrazioni di assicurare la sicurezza dei dati, dei sistemi, delle infrastrutture e delle reti nel rispetto delle regole tecniche previste dal CAD (regole tecniche cui si rinvia), nel caso che la soluzione di Disaster recovery sia realizzata tramite l'acquisizione di un servizio prestato da un fornitore si sottolinea che è consigliabile, sulla base delle modalità di backup individuate, che la componente legata alla connettività venga inserita come elemento della soluzione di DR, piuttosto che come servizio a sé stante, fatta salva le preventiva verifica dell'eventuale disponibilità nel SPC.

Una soluzione di rete per un servizio di Disaster recovery dovrebbe avere come requisito primario la presenza di un doppio percorso alternativo tra i centri connessi, garantito contrattualmente dal provider, per evitare un punto di minore affidabilità della soluzione complessiva dovuto proprio a questa componente.

Vi è peraltro da dire anche che, sebbene il "doppio percorso" sia uno dei metodi realizzativi più comuni per ottenere alta affidabilità del collegamento, una valutazione generale della connettività deve tener conto anche dei parametri di servizio, indipendentemente dalla modalità di realizzazione degli stessi, quali ad es:

- disponibilità;
- tasso d'errore;
- tempo di attraversamento (latenza);
- jitter.

5 LO STUDIO DI FATTIBILITÀ E I PIANI DI CO E DI DR DELLE PA

5.1 Premessa

La precedente versione di queste Linee Guida ha dato evidenza, in questo capitolo, della struttura generale che lo studio di fattibilità tecnica (SFT) avrebbe dovuto rispettare in occasione della presentazione della richiesta di parere da parte delle Amministrazioni.
Il capitolo, inoltre, forniva alcune sintetiche indicazioni circa i contenuti del piano di continuità ICT (ne l presente documento già indicato anche come PCO) e del piano di disaster recovery, ai quali fa esplicito riferimento l'articolo 50-bis.
In merito al primo aspetto (i contenuti dello studio di fattibilità tecnica), i contenuti generali dello SFT sono stati inseriti nella circolare n. 58 di DigitPA del 1° dicembre 2011, più volte richiamata nelle presenti Linee Guida.

Inoltre, allo scopo di aiutare le Amministrazioni a predisporre lo SFT, DigitPA (oggi Agenzia per l'Italia Digitale) ha messo a disposizione, successivamente alla pubblicazione delle Linee Guida e della citata circolare n. 58, un modello generale di studio di fattibilità tecnica. L'esperienza derivante dalle numerose richieste di parere ha dimostrato la sostanziale efficacia del modello indicato, che non ha presentato, nella compilazione, particolari difficoltà, superato, naturalmente, un periodo iniziale di avviamento dei processi legati all'attuazione della norma.
Nella presente revisione si intende inserire il modello dello studio di fattibilità tecnica al posto delle indicazioni generiche sui suoi contenuti. Si vuole anche cogliere occasione per inserire alcune aggiunte allo stesso che si ritengono necessarie sia per permettere alle pubbliche amministrazioni di meglio precisare il proprio percorso verso la continuità operativa ICT dei propri servizi, sia per consentire all'Agenzia una comprensione più completa di questo percorso. Per dare evidenza a queste aggiunte, rispetto al modello iniziale, queste saranno evidenziate da uno sfondo grigio. La validità del modello di SFT così integrato avrà valore dalla data di pubblicazione della presente revisione delle Linee Guida.

Quanto all'altro contenuto del capitolo, le sintetiche indicazioni del piano di continuità operativa (ICT) e del piano di disaster recovery, va sottolineato che molte Amministrazioni, ottenuto il parere sullo SFT, hanno manifestato all'Agenzia l'esigenza di disporre di un riferimento anche per questi piani. Si tratta di un'esigenza alla quale risulta difficile dare piena risposta.
Infatti, come peraltro già evidenziato nella versione originaria delle Linee Guida, il piano di continuità operativa, anche se ristretto alla componente ICT, può articolarsi, in relazione alle dimensioni e alla complessità dell'organizzazione alla quale fa riferimento, in una gerarchia documentale che non è possibile generalizzare.
Per dare, in ogni caso, un aiuto ad Amministrazioni che trovassero maggiori difficoltà nel predisporre questo piano, ma la cui struttura non abbia particolari complessità o dimensioni, viene riportato in appendice un modello di "Piano di Continuità Operativa ICT".
Tale modello:
- include la componente del disaster recovery, come specificato nel modello stesso;
- non rappresenta un riferimento obbligato per le pubbliche amministrazioni, che possono quindi utilizzare impianti differenti.

Il modello è stato pensato come elemento di continuità con i contenuti dello SFT e del parere successivamente emesso; il modello, infatti, ha come elementi di ingresso i servizi e le relative valutazioni di criticità che le Amministrazioni hanno identificato in fase di predisposizione dello

SFT e le successive osservazioni e richieste contenute nei pareri conseguenti. Pertanto, il modello perde molta parte della sua utilità in assenza del precedente percorso (SFT, parere).

Inoltre, l'Agenzia ritiene che, indipendentemente dal modello di piano di continuità ICT adottato, quindi, anche indipendentemente dalle dimensioni di un'Amministrazione, la suddetta visione (la continuità dei servizi come elemento centrale del piano) sia fortemente richiesta e che, quindi, anche in presenza di un percorso che abbia previsto la BIA e l'analisi del rischio e che produca PCO/PDR più complessi e articolati di quello del modello presente, ogni contenuto del piano di continuità ICT sia collegato ai servizi evidenziati (e/o modificati/integrati successivamente allo SFT) dall'Amministrazione. Infatti, la perdita di visione dei servizi come elemento centrale per la continuità nelle pubbliche amministrazioni vanificherebbe il lavoro che le Amministrazioni hanno condotto per la predisposizione dello Studio di fattibilità Tecnica.
Il Piano di Continuità Operativa ICT (PCO) e il Piano di DR possono essere inclusi in un unico documento che riporti sia le caratteristiche organizzative e procedurali per la gestione delle emergenze informatiche, sia le componenti infrastrutturali (data center, sistemi di elaborazione e di storage, software di sistema e applicativo, ecc.) ed è questa l'assunzione che è stata fatta nello sviluppare il modello in appendice. In realtà particolarmente complesse, all'opposto, il Piano di Continuità (PCO) può essere solo un documento di primo livello, cui vanno associati, per esempio, documenti di secondo livello, a cominciare dal Piano di DR e dalle 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.

È di fondamentale importanza che tutta la documentazione relativa al PCO sia stata già approvata dalla dirigenza dell'Amministrazione, soprattutto la documentazione che conferisce gli opportuni poteri e responsabilità alle varie figure (Comitato di Crisi ICT, Responsabile della Continuità Operativa) durante la fase di emergenza.

Il PCO si compone di attività e fasi che devono essere dettagliatamente specificate e descritte. É utile in ogni caso avere una visione complessiva dell'intero flusso di attività in modo che ciascun soggetto coinvolto abbia immediatamente evidenza delle interazioni tra le singole fasi.

Il PCO rappresenta pertanto la guida che indica come reagire ad eventi "negativi" di significativa rilevanza, che determinano l'indisponibilità di quei processi/servizi critici di cui si garantisce il ripristino entro determinati limiti di tempo; inoltre, prevede l'esecuzione di chiare ed efficaci azioni (formalizzate in procedure, istruzioni operative, atti e documenti), da parte dei soggetti coinvolti nel piano, come completa risposta alla situazione d'emergenza, finalizzate al ripristino dei servizi sino al rientro alla situazione di normalità.

Tali azioni dovranno essere eseguite da ciascun soggetto con immediatezza, in considerazione degli obiettivi da perseguire. Inoltre, nell'ambito della struttura organizzativa per il PCO predisposto dall'Amministrazione, il Responsabile della Continuità Operativa assume un ruolo strategico, sia in condizioni ordinarie, sia in eventuali condizioni di emergenza, per assicurare il coordinamento delle operazioni e il mantenimento, aggiornamento e sviluppo futuro del piano.

5.2 Lo Studio di Fattibilità Tecnica: modello di riferimento

In questo paragrafo si illustra il modello di riferimento che viene utilizzato per la compilazione dello SFT da sottoporre all'Agenzia, al termine della fase di autovalutazione eseguita, secondo quanto illustrato nel precedente capitolo, con l'impiego del tool reso disponibile dall'Agenzia.

Resta fermo che lo SFT deve essere compilato dalla singola Amministrazione e presentato dal "Responsabile della Continuità Operativa" (di cui si è trattato nel precedente capitolo); nel caso di

una Amministrazione articolata in diverse strutture che operano sostanzialmente in modo autonomo, si raccomanda di ricercare al massimo la possibilità di predisporre un unico SFT, eventualmente, per facilità di presentazione, suddividendolo in capitoli, ognuno relativo all'area che, per varie ragioni, quali diversità o specificità all'interno della complessiva Amministrazione, ha predisposto una propria valutazione delle criticità e un proprio, autonomo percorso per la realizzazione della continuità operativa dei servizi.

L'esperienza delle molteplici situazioni che devono essere considerate, ha però dimostrato che esistono casi in cui non è possibile predisporre un unico SFT, come, a esempio, può avvenire in ministeri che hanno accorpato precedenti strutture o nativamente includano varie strutture sotto forma di dipartimenti, strutture di dimensioni rilevanti e completamente differenti sotto il profilo delle finalità istituzionali e in molti casi anche sotto il profilo della infrastruttura tecnologica a loro supporto. Per questi casi, al fine di impedire che la mancanza di alcune componenti amministrative porti alla mancata ottemperanza della norma anche da parte di settori delle Amministrazioni che, invece, siano in grado di predisporre un proprio SFT "locale", si suggerisce alle Amministrazioni di procedere alla predisposizione dello SFT, motivando, come indicato nella presentazione del modello, la non unicità del documento rispetto all'intera organizzazione amministrativa di appartenenza. In questo caso le strutture organizzative e tecniche, a cominciare dal Responsabile della CO ICT, dovranno essere riferite alla soluzione o alle soluzioni contenute nello SFT.
Resta, infine, la necessità che anche Amministrazioni che già dispongono di una soluzione attiva di continuità predispongano lo SFT e richiedano il relativo parere.

Fatte queste premesse, il modello generale di SFT è di seguito rappresentato, con le indicazioni, come detto, delle aggiunte. Nel modello che segue, le espressioni evidenziate in corsivo rappresentano indicazioni e/o commenti alle varie sezioni del modello di SFT e non i contenuti richiesti del documento.

INTRODUZIONE
In questo capitolo vengono inseriti i richiami alle norme rilevanti. Per omogeneità editoriale degli Studi di fattibilità tecnica (SFT) il testo del capitolo 1 che segue è proposto per tutte le Amministrazioni:

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 PPAA 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 [oggi Agenzia per l'Italia Digitale], 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 [oggi Agenzia per l'Italia Digitale].

OBIETTIVI DEL DOCUMENTO

In ottemperanza a quanto citato nel punto 4 dell'articolo 50bis del CAD viene redatto il presente documento di SFT per poter dare evidenza dei risultati emersi nel percorso di autovalutazione, illustrando tra le altre cose:

- gli eventuali scostamenti tra la soluzione individuata al termine del percorso di autovalutazione e quella effettivamente scelta dalla Amministrazione;
- il percorso e i tempi che si stima siano necessari per adottare la soluzione suggerita al termine del percorso di autovalutazione e per allinearsi a quanto previsto dalle Linee Guida.

Il documento si prefigge quindi di fornire all'Agenzia per l'Italia Digitale le informazioni necessarie e propedeutiche alla realizzazione del piano di disaster recovery come parte integrante del più ampio piano di continuità operativa.

Quale raccomandazione generale, relativamente alla selezione dei servizi oggetto dell'autovalutazione, si consiglia di utilizzare il criterio dei servizi "esposti al pubblico", cioè quelli che offrono le proprie funzionalità a utenti finali (cittadini, imprese, altre PA, utenti interni all'Amministrazione). I servizi tecnici IT, invece, quali, a esempio, i servizi di AAA, Autenticazione, Autorizzazione ed Accounting, sono infatti utilizzati da utenti intermedi (ad esempio gli sviluppatori sw o i sistemisti) o sono precondizione per il funzionamento dei servizi destinati al pubblico come sopra definiti.

CONTENUTI DEL DOCUMENTO

INFORMAZIONI GENERALI

In questo capitolo vanno riportate le informazioni generali dell'Amministrazione che ha redatto lo SFT.

Nome Amministrazione	
Sede centrale (città)	
Settore di attività	
Responsabile CO/DR	
AOO (Area Org. Omog.)/ENTE	
Indirizzo PEC per le comunicazioni	
Data compilazione	
Perimetro di competenza del presente SFT	*Indicare se il presente SFT è relativo a tutte le aree dell'Amministrazione. Se non lo è, deve essere precisato quali Dipartimenti, Direzioni, Aree, Uffici, ecc. sono stati oggetto dello SFT e deve essere esplicitata la motivazione per la quale l'Amministrazione ha ristretto ai settori indicati lo SFT.*

Descrizione dell'Amministrazione, organizzazione e funzioni istituzionali

Inserire una descrizione discorsiva dell'Amministrazione, che, almeno, contenga il ruolo istituzionale e la propria organizzazione interna di alto livello (ad esempio uffici e/o dipartimenti/delegazioni).
Dopo tale descrizione, riportare una tabella, strutturata per Uffici competenti sui servizi di seguito rappresentati, del tipo:

NOME SERVIZIO	UFFICIO COMPETENTE	NOME RESPONSABILE UFFICIO

L'AMBITO DELLO STUDIO DI FATTIBILITÀ TECNICA

In questo capitolo va descritto l'ambito in cui si applica lo SFT, ossia il complesso dei servizi e della relativa struttura che li eroga, per i quali lo SFT propone la soluzione per la continuità operativa ICT e DR.

SERVIZI EROGATI

Servizi in Ambito

In questo paragrafo vanno inseriti tutti i servizi erogati che verranno coperti dalla soluzione che si intenderà adottare. E' opportuno avvalersi della tabella che segue.
Sarebbe opportuno che si effettui un raggruppamento in classi omogenee dei servizi aventi caratteristiche comuni, nel qual caso le autovalutazioni e i tipi di soluzioni si riferiranno alla classe e non al singolo servizio. Le classi di servizi o i servizi devono essere gli stessi per i quali è stata redatta l'autovalutazione tramite lo strumento. Nel caso di utilizzo di classi di servizio è opportuno che, per ognuna di esse, venga riportata una breve descrizione dei criteri adottati per il raggruppamento.

Nel campo "Tipologia" di Utenza va inserita la stessa tipologia utilizzata nella compilazione della corrispondente scheda di autovalutazione.

Classe di Servizi	Servizio	Descrizione Servizio	Tipologia di Utenza

Servizi non in Ambito

In questo paragrafo devono essere riportati eventuali servizi che l'Amministrazione ha ritenuto tenere al di fuori dell'ambito dello SFT. Si richiede però, in ogni caso:

- *la valutazione della criticità del servizio non in ambito;*
- *le motivazioni dell'esclusione del servizio dall'ambito della/e soluzione/i di continuità ICT*

Servizio	Descrizione Servizio	Tipologia di Utenza	Classe di criticità	Motivazione dell'esclusione dall'ambito della soluzione/i di continuità dei servizi

Descrizione dettagliata Servizi/Classe di Servizi

In questo paragrafo va inserito il riferimento all'allegato o agli allegati in cui sono riportati i file prodotti dallo strumento di autovalutazione. Il testo che segue è proposto come esempio:

Per ogni servizio o classe di servizi che fa parte dell'ambito dello Studio di Fattibilità Tecnica è stata redatta una scheda di autovalutazione, i cui risultati sono riportati negli allegati *Allegato1: Schede xxx, Allegato2: Schede yyy* al presente documento.

IL RISULTATO DEL PERCORSO DI AUTOVALUTAZIONE

In questo capitolo, per ogni servizio/classe di servizi che fa parte dell'ambito dello Studio di Fattibilità Tecnica, già descritti nel paragrafo 3.1.1, devono essere riportati i dati emersi nel corso dell'autovalutazione e che sono riportati nello schema di sintesi dell'autovalutazione, dando anche evidenza dei valori di RPO ("Tempo massimo tollerabile tra la produzione di un dato e il suo salvataggio" nel tool di autovalutazione) e di RTO ("Tempo massimo tollerabile di indisponibilità del servizio" nel tool di autovalutazione):

Servizio/ Classe di Servizi	Indice complessivo di criticità	Classe di criticità	Soluzione tecnologica (Tier)	RPO da autovalutazione	RTO da autovalutazione

LA/LE SOLUZIONE/I TECNOLOGICA/CHE E TECNICA/CHE

In questo capitolo va indicato il dettaglio della soluzione o delle soluzioni che l'Amministrazione ha individuato come rispondente/i alle proprie esigenze. Il capitolo va compilato anche nel caso in cui la soluzione (o le soluzioni) sia/siano già in essere oppure siano già stati redatti il piano di continuità operativo e/o il piano di DR relativi.

*È necessario porre attenzione alla terminologia a cui si fa riferimento. Si parlerà di "**soluzione tecnologica**" quando ci si vuol riferire alla classificazione (Tier 1…Tier 6) in analogia a come viene*

*utilizzata nelle Linee Guida (LG) e nello strumento di autovalutazione. Ogni soluzione tecnologica potrebbe essere realizzata secondo una o più "**soluzioni tecniche**". I nomi delle soluzioni tecniche sono a discrezione dell'estensore dello studio. È necessario però che tale nome sia univoco. Quindi la "**soluzione**" sarà individuata dalla soluzione tecnologica e dalla soluzione tecnica: ad esempio "Tier3/soluzione tecnica A".*

Soluzione adottata o da adottare

*Nel caso sia stata individuata una sola soluzione dovrebbe essere riportata la seguente frase: "*Tutti i servizi in ambito sono coperti da una sola soluzione tecnica che fa riferimento alla soluzione tecnologica di tipo Tier x" *dove x è un valore cha può andare da 1 a 6.*

Nel caso siano state individuate più "soluzioni tecnologiche" deve essere compilata una tabella (composta da tante righe quante sono le soluzioni tecnologiche) che metta in evidenza quali servizi siano coperti dalla singola soluzione tecnologica.

Soluzione tecnologica	Servizi/classi di servizi coperti
Tier x	servizio 1
	servizio 2
Tier y	Classe di servizio 1

Sintesi delle soluzioni tecnologiche e tecniche

In questo paragrafo devono essere descritti gli elementi qualificanti per l'implementazione della soluzione tecnologica e/o delle soluzioni tecnologiche indicate nel paragrafo precedente e delle eventuali soluzioni tecniche relative (una o più), avuto riguardo a tutto quanto attiene al perimetro della Continuità Operativa ICT delineato nel capitolo 1 delle LG. (creare un sottoparagrafo per ogni soluzione tecnologica che si intende adottare).

Per ogni soluzione che verrà indicata è NECESSARIO che l'Amministrazione dichiari i valori di RTO e di RPO della soluzione stessa. Nel caso che uno o entrambi di questi valori fossero peggiorativi rispetto ai valori di RTO e RPO come determinati dall'autovalutazione anche di uno soltanto dei servizi ai quali la soluzione si riferisce, è NECESSARIO che l'Amministrazione motivi questa difformità.

Nel caso in cui si descrivano soluzioni non ancora in essere, o per le quali non siano stati redatti il piano di continuità operativa e/o piano di disaster recovery, va indicato se quanto verrà descritto fa riferimento a stime o a scelte già consolidate.

Nel caso in cui la soluzione tecnologica e/o tecnica sia realizzata da fornitori o da altra Amministrazione, è necessario che vengano riportati il dettaglio di tutti i requisiti contrattuali.

Per ogni soluzione tecnica relativa alla stessa soluzione tecnologica, sarà necessario redigere una o più tabelle (in caso di più soluzioni tecniche per una soluzione tecnologica) con i seguenti contenuti:

Soluzione	*Indicare: "Soluzione Tecnologica/Soluzione Tecnica" (ad es: Tier3/Soluzione Tecnica A)*
Stato della soluzione	*Gli stati possibili: da adottare / adottata / in realizzazione*
Elenco dei servizi del Tier a cui si riferisce questa particolare soluzione	
RTO e RPO della soluzione	*Indicare i valori di RTO e di RPO della soluzione. Nel caso che tali valori fossero peggiorativi dei valori di RTO e/o di RPO anche per uno solo dei servizi ai quali la soluzione si riferisce, è necessario motivare la ragione di tale difformità.*

Gestione infrastruttura IT del/dei sito/i di produzione per i servizi afferenti alla soluzione	*Indicare una delle scelte tra parentesi per ognuno dei servizi afferenti alla soluzione: (interna, esterna (in questo caso indicare gli elementi minimi contrattuali: durata, LDS, localizzazione sito): presso fornitore, presso società in house/centro servizi, presso altra Amministrazione)* *Se esistono infrastrutture differenti per i servizi, sia afferenti alla soluzione considerata, sia riferiti ad altre soluzioni, indicarlo (ma senza specificare le differenze)* *In ogni caso, devono essere indicati l'indirizzo (o gli indirizzi) del sito (o dei siti) presso i quali vengono eserciti i servizi di questa soluzione.*
Gestione della soluzione per il/i sito/i di DR per i servizi afferenti alla soluzione	*Indicare una delle scelte tra parentesi per ognuno dei servizi afferenti alla soluzione: (interna, esterna: presso fornitore, presso società in house/centro servizi, presso altra Amministrazione)* *Se esistono infrastrutture differenti per i servizi, sia afferenti alla soluzione considerata, sia riferiti ad altre soluzioni, indicarlo (ma senza specificare le differenze)*
Le caratteristiche della/e soluzione/i di DR sono conformi alle "Linee guida per il DR delle PA"	*Evidenziare eventuali difformità e relative motivazioni OPPURE dichiarare esplicitamente la conformità*
Descrizione dell'organizzazione per la gestione delle emergenze che si intende adottare (per esempio, come indicato nel capitolo 3 delle "Linee guida per il DR delle PA").	*Descrizione.* *Se comune con altre soluzioni, indicarlo esplicitamente*
Distanza in km prevista tra il sito principale e il sito di DR	
Trasferimento dati tra siti: quanti dati vengono trasferiti (GB, TB) relativamente ai servizi afferenti alla soluzione	*Espressa in GB o TB, così suddivisi:* *Trasferimenti giornalieri (in GB/TB)* *Trasferimenti settimanali (in GB/TB)* *Trasferimenti mensili (in GB/TB)*
Trasferimento dati tra siti: indicare se vengono trasferiti dati sensibili e/o giudiziari relativamente ai servizi afferenti alla soluzione	*Se sì, indicare "sensibili e/o giudiziari"*
Modalità di trasferimento dati tra siti	*Indicare:* *a) se solo trasferimento, indicare quali supporti e la frequenza di trasferimento;* *b) se trasmissione on line, indicare banda garantita e % banda utilizzata*
Tipologia di risorsa elaborativa nel sito primario	*Utilizzare una delle scelte tra parentesi (fisica, virtualizzata, mista)*
Risorse elaborative previste nel sito secondario	*Utilizzare una delle scelte tra parentesi (equivalenti a quelle nel primario o ridotte in termini di prestazioni; condivise o dedicate)* *Se ridotte, esplicitare la motivazione*
Dimensioni dello storage nel sito primario e secondario relativo ai servizi afferenti alla soluzione	*Espresse in GB o TB*
Connettività del sito DR con eventuali sedi periferiche	*Indicare se: "esiste / è prevista / non è prevista"*

Numero minimo di PDL per garantire la funzionalità di servizi offerti	*Indicare il numero di postazioni necessarie a garantire la funzionalità minima dei servizi offerti durante l'operatività ordinaria e l'operatività in emergenza*
Organizzazione per la gestione di eventuali emergenze (ad es. Comitato di Crisi); se non comune con tutte le soluzioni previste, indicarlo	*Indicare se: "esiste / è prevista / non è prevista". Se esiste indicare come viene identificata e la composizione con ruoli e responsabilità*
Condizioni/rischi valutati per dichiarare lo stato di emergenza (Scenari di Crisi) relativamente ai servizi afferenti alla soluzione	*Indicare le condizioni limite affinché sia dichiarata la crisi (per attivare le misure che saranno contenute nel PCO) ed in particolare dove sono definite e documentate*
Piano di Disaster Recovery	*Indicare se già esiste un piano di DR.* *Se non unico, indicarlo*
Piano di Continuità Operativa	*Indicare se già esiste un piano di CO.* *Se non unico, indicarlo*

Riepilogo Servizi, criticità e Soluzione

Nella seguente tabella per ogni servizio/classe di servizi incluso nell'ambito SFT va riportato:

- *Servizio/classe di servizi*
- *Classe criticità, indicata dallo strumento di autovalutazione*
- *Soluzione tecnologica minima, indicata dallo strumento di autovalutazione (i possibili nomi sono Tier 1….Tier 6)*
- *Soluzione individuata: vanno riportati gli stessi nomi definiti nel paragrafo precedente (ad esempio Tier 3/Soluzione Tecnica 1, Tier 3/Soluzione Tecnica 2)*
- *Soluzione già presente (Indicare SI se la soluzione è già stata realizzata)*

Servizio / classe servizi	Classe criticità	Soluzione tecnologica minima da autovalutazione	Soluzione tecnica individuata	Soluzione già presente

Nel caso in cui soluzioni già in essere debbano essere modificate per includere nuovi servizi, è necessario che venga riportato il dettaglio.

Differenze rispetto all'autovalutazione

Per ogni servizio citato nel paragrafo precedente, se la soluzione tecnologica adottata o che si intende adottare differisce da quanto emerso dal tool di autovalutazione, in questo paragrafo è necessario riportare in dettaglio le motivazioni che hanno determinato la scelta.

TEMPI E MODALITÀ DI REALIZZAZIONE DELLA SOLUZIONE

In questo capitolo vanno riportati, per tutte le soluzioni tecnologiche e tecniche individuate, i tempi e le modalità di realizzazione. L'Amministrazione dovrà garantire il rispetto della normativa vigente in materia di appalti e garantire la necessaria apertura al mercato, ove intendesse ricorrere a fornitori esterni per dotarsi, attraverso forniture o servizi, di soluzioni di CO/DR.

Soluzione	Tempi di Realizzazione	Modalità di Realizzazione
Tier X/Soluzione Y		
Tier Y/Soluzione Z		

Tempi e Modalità Soluzioni Individuate

Deve essere riportato un piano temporale in cui si evidenzi la disponibilità di: Piano CO, Piano DR, Sito DR relativi alle singole soluzioni scelte.

Per ogni modalità di realizzazione individuata, come ad esempio: Acquisizione servizio, Forniture, Condivisione sito con altra amministrazione, Ristrutturazione sito amministrazione, devono essere descritte tutte le fasi necessarie per la loro realizzazione e il loro sviluppo temporale (eventualmente allegare GANTT delle attività).

	Data Disponibilità
Piano CO	
Piano DR	
Completamento della soluzione (collaudo effettuato, operatività della soluzione avviata)	

Vincoli e rischi Soluzione
Per ogni soluzione individuata devono essere riportati eventuali vincoli e rischi che potrebbero incidere sul piano di realizzazione, illustrando anche i tempi che si stima saranno necessari per l'adozione.

Conclusioni ed adeguatezza della Soluzione
In questo paragrafo vanno indicati tutti gli elementi aggiuntivi ai precedenti che mettano in evidenza l'adeguatezza della soluzione (delle soluzioni) prescelta.

Allegato 1: Schede XXX

Allegato 2: Schede YYY
---

6 STRUMENTI GIURIDICI E OPERATIVI PER LA ACQUISIZIONE DI UN SERVIZIO DI DR

Seguendo i metodi esaminati nei capitoli precedenti e sulla base di considerazioni di natura organizzativa, tecnica ed economica, le Amministrazioni, una volta definita la soluzione di continuità operativa più adeguata alla proprie caratteristiche, possono procedere alla sua progettazione e realizzazione anche attraverso l'acquisizione delle necessarie infrastrutture e servizi.
Anche le Amministrazioni che saranno in grado di progettare e realizzare una soluzione organizzata e gestita internamente potrebbero dover, verosimilmente, procedere all'acquisizione delle infrastrutture tecnologiche e delle risorse software necessarie a rendere operativi il PCO e il PDR adottati.
Le metodologie e le soluzioni di CO e di DR presentate nei capitoli che precedono sono tutte diversamente caratterizzate da elementi di complessità che, in sede di richiesta al mercato ed affidamento contrattuale, necessitano di una corretta *governance* da parte dell'Amministrazione richiedente.
Proprio la complessità di queste tematiche, inoltre, può rendere conveniente il ricorso a politiche di co-gestione delle soluzioni di CO e di DR tra più Amministrazioni omogenee per struttura, organizzazione e ubicazione geografica; l'associazione di più Amministrazioni può anche essere realizzata utilizzando, in tutto o in parte, le infrastrutture esistenti presso le singole Amministrazioni partecipanti all'associazione. Tale modalità è quella definita come "mutuo soccorso".

In questo capitolo vengono forniti una serie di suggerimenti e indicazioni in merito alle modalità di approvvigionamento delle forniture e dei servizi necessari alla realizzazione delle soluzione di DR individuate.

Alla luce del lavoro svolto dal Tavolo tecnico a ciò deputato, sono anche individuati i servizi minimi essenziali per l'adozione delle soluzioni di DR (schede servizi), esempi di possibile combinazione di dette schede per i vari casi, nonché 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.).

6.1 I possibili servizi minimi essenziali

Scopo del presente paragrafo è quello di richiamare i servizi minimi essenziali per le soluzioni di DR e deriva dal lavoro svolto dal tavolo tecnico all'uopo istituito dall'Agenzia per l'Italia.

Il capitolo, che non intende elencare tutte le forniture e servizi informatici che si possono reperire sul mercato né intende essere esaustivo in merito alle possibili combinazioni che si possono adottare, definisce delle "schede di servizio" che possono essere utilizzate da tutte le PPAA sia centrali, sia locali, per rivolgersi ai fornitori, al fine di richiedere i servizi necessari per dotarsi di soluzioni di DR o anche per migliorare quelle esistenti. Le schede, che descrivono i servizi minimi essenziali e i loro relativi sottoservizi, (riportate nel dettaglio sul sito istituzionale dell'Agenzia, nel documento *"I SERVIZI MINIMI ESSENZIALI PER L'ADOZIONE DELLE SOLUZIONI DI DISASTER RECOVERY"*reperibile al link: http://www.digitpa.gov.it/sites/default/files/Raccomandazioni_PROFILI%20MINIMI%20SERVIZI%20DI%20DR_v_2_4_0.pdf) possono essere riassunte come segue:

LISTA SERVIZI	BREVE DESCRIZIONE E SOTTOSERVIZI
D1: Supporto alla predisposizione della documentazione per l'acquisizione del parere ai sensi del c. 4, dell'art. 50bis del CAD	Servizi di consulenza e supporto alla redazione della documentazione necessaria alla richiesta di parere. Sottoservizi: A.Supporto per: -la compilazione delle schede di autovalutazione; -la predisposizione dello Studio di Fattibilità Tecnica; -la predisposizione della Relazione Tecnica sullo stato di attuazione del CAD. B. Consulenza per Business Impact Analysis (BIA): Individuazione e valutazione servizi critici per la sopravvivenza del business; C. Consulenza per Risk Assessment (RA): Valutazione
D2: Servizio di Predisposizione dei piani di CO/DR e di progettazione organizzativa/procedurale e tecnologica della soluzione di DR"	Il servizio attiene alla produzione del piano di continuità operativa e di disaster recovery (CO/DR) partendo dallo studio di fattibilità (predisposto con la scheda D1) Sottoservizi: A.Progettazione di alto livello del modello organizzativo B.Progettazione di alto livello della soluzione tecnologica, con eventuale produzione di deliverable/studi per il consolidamento o la razionalizzazione del SI Primario (ove se ne evidenzi la necessità come passo propedeutico/prerequisito ai fini della realizzazione della soluzione di DR) C.Progettazione di dettaglio del modello organizzativo/procedurale D.Progettazione di dettaglio della soluzione tecnologica E.Redazione delle procedure di DR F.Redazione del piano di CO
D3: Il sito di DR: aree CED e aree attrezzate per posti di lavoro	Disponibilità e mantenimento di aree CED e aree per PdL, nel quale siano installati o installabili i sistemi necessari a ripristinare i servizi informatici identificati nello Studio di Fattibilità e dettagliati nel progetto esecutivo. Il servizio potrà articolarsi nei seguenti sotto-servizi: A. Disponibilità della struttura edile e impiantistica per gli spazi del sito di DR B. Esecuzione degli eventuali interventi sul sito primario e sul sito di DR comprensiva, ove necessario, della predisposizione dell'infrastruttura tecnico-logistica, per renderlo conforme ai requisiti minimi obbligatori riportati in allegato alla presente scheda D3, definiti – a seguito dei servizi di progettazione della scheda D2 – come passo propedeutico/prerequisito della realizzazione della soluzione di DR C. Gestione e manutenzione del sito di DR D. Disponibilità di spazi ad uso ufficio destinati ad ospitare le PdL secondo le modalità descritte nella scheda D4 E. Gestione e manutenzione degli spazi ad uso ufficio per ospitare le PdL
D4: Componenti hw e sw della soluzione di DR	Disponibilità e manutenzione delle componenti hw e sw della soluzione di DR, in particolare: A1-A2 delle risorse elaborative hw, sw, storage necessarie alla salvaguardia dei dati e delle applicazioni e alla ripartenza presso il sito di DR A3 delle postazioni di lavoro per personale tecnico coinvolto nel processo di ripartenza e gestione del Sistema Informativo, con caratteristiche analoghe a quelle del sito temporaneamente inagibile
D5: Servizi di replica dati per il DR	Il servizio di copia e trasferimento remoto a fini di backup e restore dei dati, immagine dei sistemi, applicazioni, può avvenire con modalità diverse: •trasferimento (elettronico e non) dei supporti di back up, relativa conservazione e possibilità di riconsegna •replica via rete del contenuto dei dischi
D6: Servizi di rete per il DR	Progettazione, realizzazione, gestione e manutenzione delle componenti di rete necessarie per la soluzione di DR. Il servizio si articolerà nei seguenti sotto-servizi: A.Progettazione e dimensionamento della soluzione di rete; B.Fornitura, manutenzione e gestione, anche in modalità condivisa tra più Amministrazioni, dei componenti di rete della soluzione di DR, inclusi quelli necessari alla gestione dell'instradamento alternativo degli accessi dalla periferia in caso di emergenza

LISTA SERVIZI	BREVE DESCRIZIONE E SOTTOSERVIZI
D7: Servizi di gestione della soluzione di DR sia in condizioni di normalità che in condizioni di emergenza	Il servizio deve assicurare la gestione ottimale della soluzione di DR al fine di assicurarne la piena efficienza. Il servizio potrà essere suddiviso in due sotto servizi: A. gestione della soluzione durante la normale operatività B. gestione dell'emergenza
D8: Servizi di verifica per le soluzioni di DR	Incarichi di verifica (audit) condotti da Terza Parte Indipendente sulle diverse componenti del DR/CO; Essi possono includere l'esecuzione di uno o più dei seguenti sotto-servizi: A. verifica dei piani di DR e CO - con simulazione del disastro - senza simulazione del disastro B. verifica delle infrastrutture di DR C. verifica dei test (di simulazione del disastro) D. verifica di conformità dei processi in atto presso l'organizzazione con quelli previsti dagli standard per il DR (ad es. ISO 22301) a fini di gap analysis o di certificazione

Le schede hanno un formato comune e sono articolate indicativamente come segue:

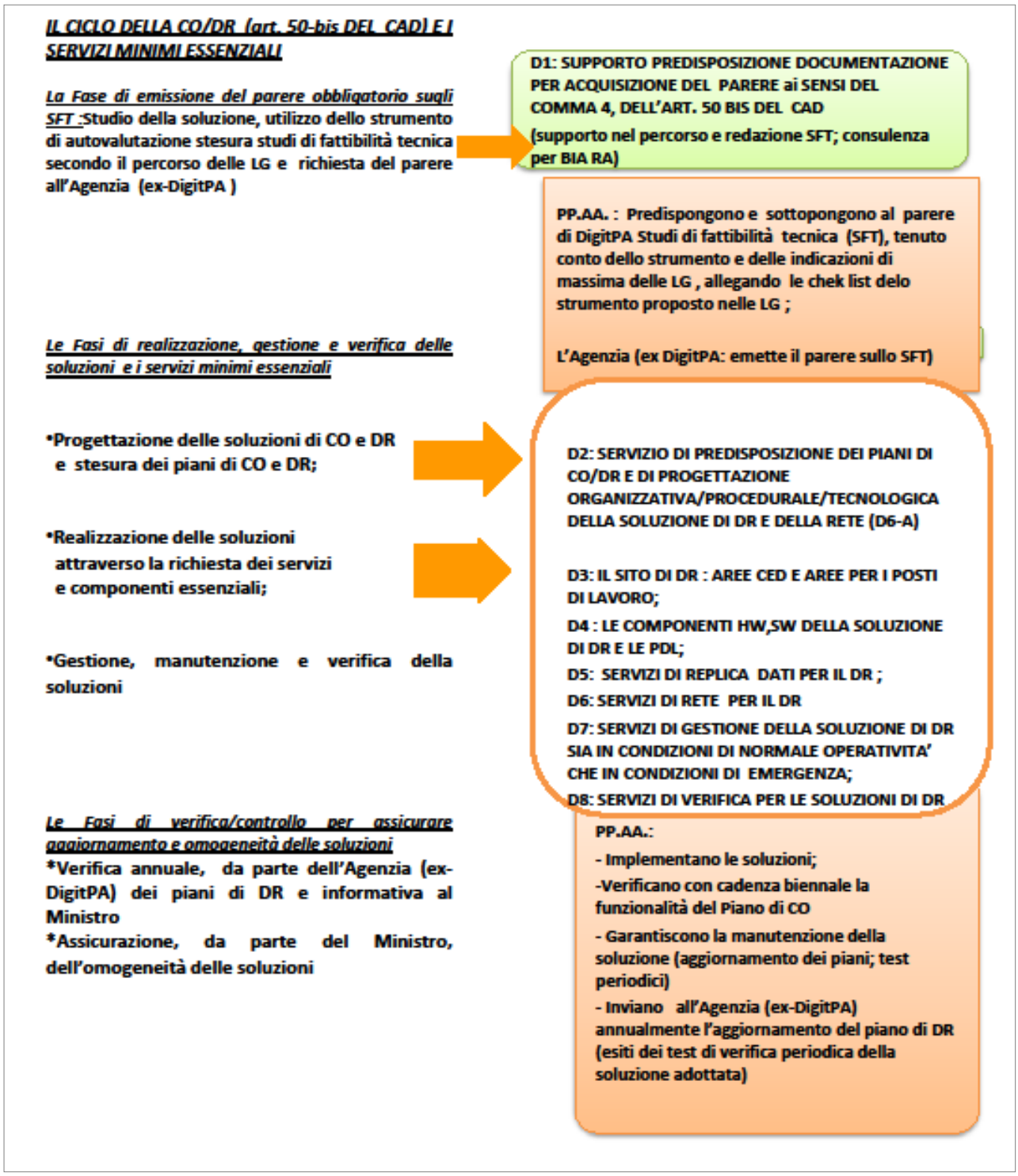
PARTE GENERALE	
DENOMINAZIONE	
DESCRIZIONE	
CORRISPONDENZA ITIL	
CORRISPONDENZA CPV	
CORRISPONDENZA con i lemmi del Dizionario delle forniture ICT DigitPA	
TIER	

PARTE TECNICA	
PRE-REQUISITI	
CARATTERISTICHE TECNICHE	
ADEMPIMENTI PREVISTI	
ADEMPIMENTI NON PREVISTI	
INDICATORI MINIMI DI SERVIZIO	
STRUMENTI DI VERIFICA DELLA CONFORMITÀ DEL SERVIZIO	
COMPETENZE RICHIESTE	
TEMPI DI REALIZZAZIONE	

PARTE ECONOMICA (Componenti di costo)	
COSTI UNA TANTUM	
COSTI PERIODICI	
COSTI DI EVENTUALI ATTIVITÀ AGGIUNTIVE	

I servizi descritti dalle schede possono avere una precisa collocazione nell'iter prefigurato dall'art. 50bis del CAD.

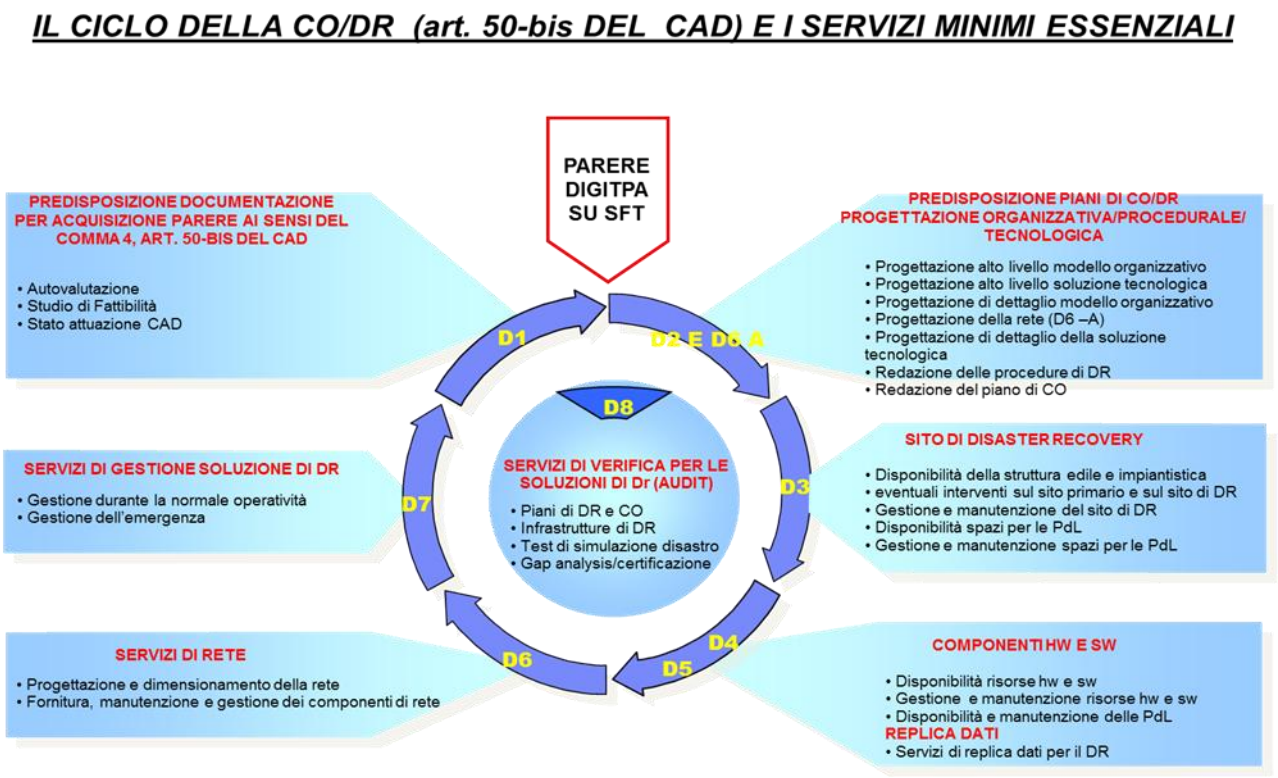
In particolare, per le Amministrazioni che devono avviare il processo completo, a partire dalle attività per la predisposizione della richiesta di parere sullo studio di fattibilità tecnica della soluzione di DR, fino ai servizi di disponibilità del sito di DR e delle risorse elaborative con le relative attività di gestione, la collocazione dei servizi rispetto alle varie fasi previste dall'art. 50bis del CAD può essere rappresentata come nella seguente figura.



Collocazione dei servizi descritti dalle schede all'interno dell'iter prefigurato dall' art. 50bis del CAD.

La figura seguente sintetizza l'impiego dei vari servizi nel ciclo più generale dell'attuazione della CO e delle soluzioni di DR.

Il ciclo della CO/DR



Le schede precedentemente descritte potranno esser utilizzate dalle Amministrazioni che hanno inteso adottare le soluzioni accennate, a titolo esemplificativo, nel seguente modo.

Si prenda il caso di un'Amministrazione che debba partire ex novo nell'attuazione di quanto disposto dall'art. 50bis, ricorrendo a fornitori esterni: essa potrà attingere ai servizi di supporto e progettazione delle schede D1 e D2 e se al termine del percorso effettuato con il tool di autovalutazione e il supporto del fornitore, intenderà garantire la salvaguardia dei dati e delle applicazioni con soluzione Tier 3, dovrà dotarsi di un sito con le caratteristiche indicate nella scheda D3, delle componenti hardware e software e di rete, richiamate nelle schede D4 e D6 e replicare i dati secondo le modalità descritte nella scheda D5. Laddove intendesse poi affidare in outsourcing la gestione della soluzione di DR, potrà attingere a servizi come quelli descritti nella scheda D7.

Si prenda altresì il caso di un'Amministrazione che già disponga di un soluzione di DR del tipo Tier 2, con un sito alternativo e un servizio di esecuzione e conservazione delle copie di backup dei propri dati e applicazioni. Se la stessa volesse verificare l'adeguatezza della soluzione di DR in essere, anche perché, ad esempio si è esteso il numero di procedimenti svolti esclusivamente in modalità informatica o perché il quadro normativo ha ampliato il proprio asset di servizi e processi critici, la stessa potrà decidere di eseguire una nuova BIA o RA, attingendo ai sottoservizi della scheda D1, e eventualmente, una volta deciso di aggiornare la soluzione in essere, passando ad una soluzione Tier

3, potrà attingere ai servizi e componenti della scheda D6, dotandosi dei servizi di rete per il DR ed eventualmente dei servizi di gestione della scheda D7 precedentemente citata.

Si prenda il caso di Amministrazioni che già dispongono di soluzioni e servizi di DR volessero farsi coadiuvare nella proprie attività di controllo e monitoraggio dell'adeguatezza della soluzione, possono attingere a fornitori a ciò qualificati per i servizi di verifica delle soluzione di DR, come declinato nella scheda D8.

Altro caso, emerso dall'esperienza maturata nel primo periodo di attuazione dell'art. 50bis: l'Istituto scolastico che debba dotarsi di una soluzione Tier 1, con 1 server e 10 PDL, con trasferimento settimanale dei supporti dati in sede secondaria o di altro istituto e con accordo con il fornitore per installazione server in caso emergenza, potrà attingere ai servizi di supporto e progettazione delle schede D1 e D2, verificare che il sito abbia le caratteristiche indicate nella scheda D3, nonché curare di approvvigionarsi dei servizi di replica e trasferimento remoto di backup e restore previsti nella scheda D5 e prevedere in apposito contratto che, in caso di emergenza, dovrà essere curata,entro i tempi di ripristino definiti, l'installazione e l'attivazione dei server.

Infine, si prenda l'esempio di Comuni che debbano adottare una soluzione Tier 3 e che già dispongano di collegamenti fra le sedi del sito primario e secondario tramite VPN, su rete SPC: essi dovranno assicurasi che il sito secondario abbia le caratteristiche indicate nella scheda D3 e regolamentare adeguatamente nell'accordo di mutuo soccorso, per garantirsi la corretta condivisione delle risorse.
Laddove poi volessero farsi supportare nella verifica dell'adeguatezza delle soluzioni dette Amministrazioni locali potranno anche attingere, verificate le relative disponibilità di budget, dei servizi di verifica per le soluzioni di DR della scheda D8.

6.2 Possibili percorsi per l'attuazione di soluzioni di CO e di DR

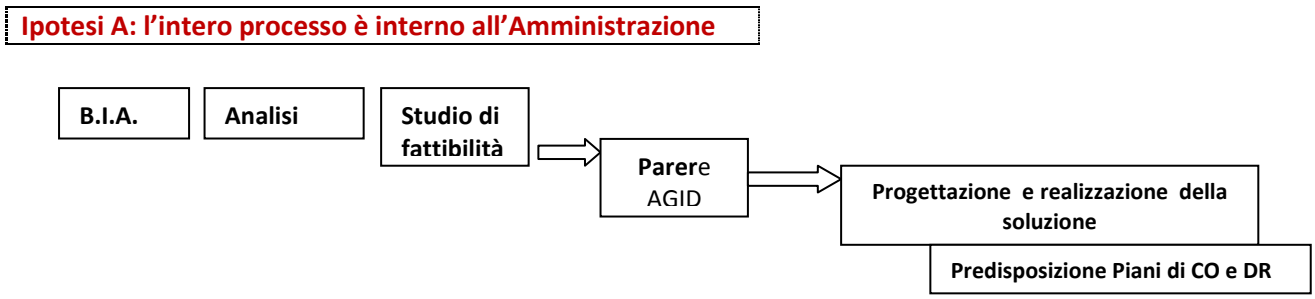
Le soluzioni e ipotesi che si possono percorrere per l'attuazione di una soluzione di CO e di DR sono di seguito schematicamente descritti nelle linee generali: la composizione dei beni e servizi che possono dover essere acquisiti da una PA dipende essenzialmente dalla soluzione di continuità operativa che l'Amministrazione stessa ritiene più opportuno adottare a livello tecnico ed operativo, sulla base del percorso in precedenza illustrato, partendo quindi dal proprio contesto tecnico-operativo, dalla criticità e portata per l'utenza dei dati e dei servizi resi, dagli esiti della BIA e dell'analisi Costi/Benefici effettuate (nei disegni di seguito riportati sinteticamente richiamata con l'acronimo C.B.).

Per il contesto di riferimento e le finalità delle presenti Linee Guida, sono state ipotizzati differenti esempi, puramente indicativi, dei possibili percorsi per l'acquisizione delle soluzioni di CO e di DR.

Nei casi in cui una Amministrazione debba dotarsi di una soluzione di CO e di DR e non disponga, in tutto o in parte, al proprio interno del sito, delle componenti hw e sw, delle risorse professionali necessarie, può ricorrere ad un prestatore di servizi ICT – a seconda dei casi per tutte o parte delle fasi di progettazione, implementazione e realizzazione di una soluzione di CO e di DR, attuando, ad esempio i percorsi descritti nelle ipotesi di seguito riportate.

6.2.1 Ipotesi A: percorso di attuazione della soluzione di CO e DR interno all'Amministrazione

In questo caso l'Amministrazione potrà avere bisogno unicamente di ricorrere al mercato per acquisire HW e SW necessario alla realizzazione del piano adottato, con gli ordinari strumenti giuridici e nel rispetto dei presupposti di Legge.



6.2.2 Ipotesi B: percorso di attuazione della soluzione di CO e DR con il supporto parziale di fornitori

Di tutta evidenza, in questo caso, la necessità di una preliminare ed accurata ricognizione del contesto tecnico che connota il Sistema Informativo primario per il quale deve essere progettata la soluzione.
Al termine della fase di ricognizione si ritiene opportuno che il fornitore metta a disposizione apposito documento contenente gli esiti della ricognizione effettuata con dettagliata descrizione delle caratteristiche e della dimensione:

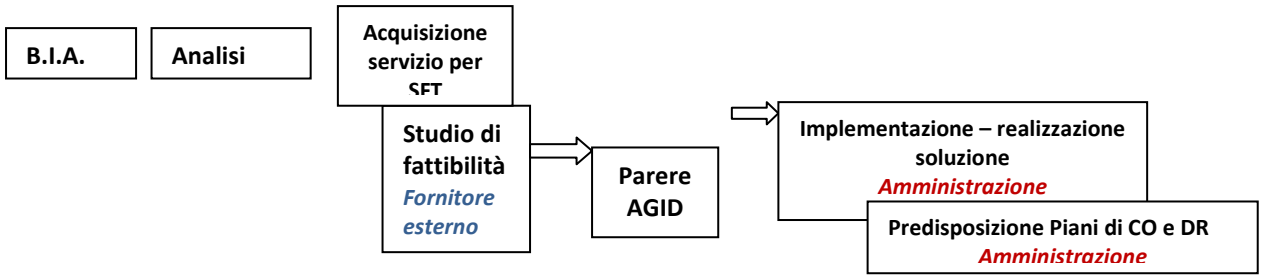
- delle componenti HW, SW e di rete dell'architettura del Sistema Informativo;
- delle applicazioni e delle basi di dati;
- delle funzioni amministrative di competenza dell'Amministrazione;
- dei procedimenti istituzionali e strumentali che si svolgono attraverso il Sistema Informativo;
- della tipologia e ruolo dei servizi on-line erogati e degli utenti, interni ed esterni, che possono avere impatti negativi nella loro attività a fronte di eventuali fermi o disastri del Sistema Informativo.

Ai fini della ricognizione ed in vista della predisposizione del progetto per la realizzazione della soluzione, il fornitore dovrà anche verificare i vincoli tecnici e normativi conseguenti ai risultati della BIA, alle misure adottate in linea con il D. Lgs. 196/2003 e s.m.i., ovvero dalla specificità delle attività istituzionali dell'Amministrazione.

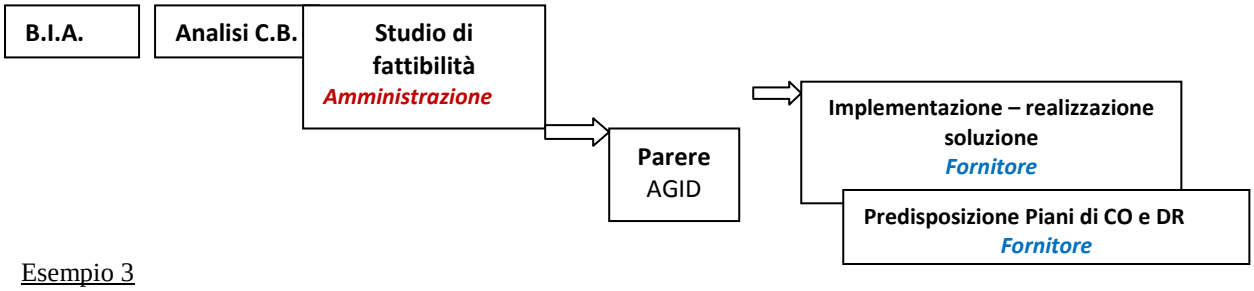
Sulla base della ricognizione effettuata ed approvata dall'Amministrazione, sarà cura del prestatore, entro i termini definiti nel piano delle attività approvato, predisporre il Progetto per la realizzazione e l'implementazione della soluzione di CO/DR, comprensivo della pianificazione, implementazione, realizzazione, collaudo e messa in esercizio, manutenzione e verifiche della soluzione proposta.

Ipotesi B: il processo è svolto dall'Amministrazione con l'acquisizione di parte del servizio (tre esempi)

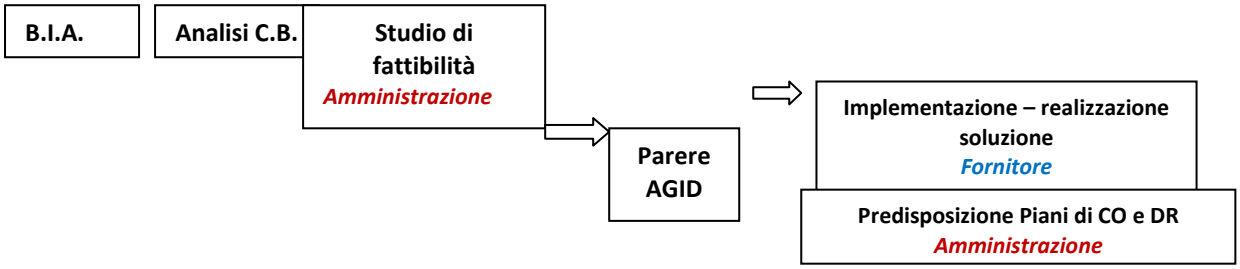
Esempio 1



Esempio 2



Esempio 3

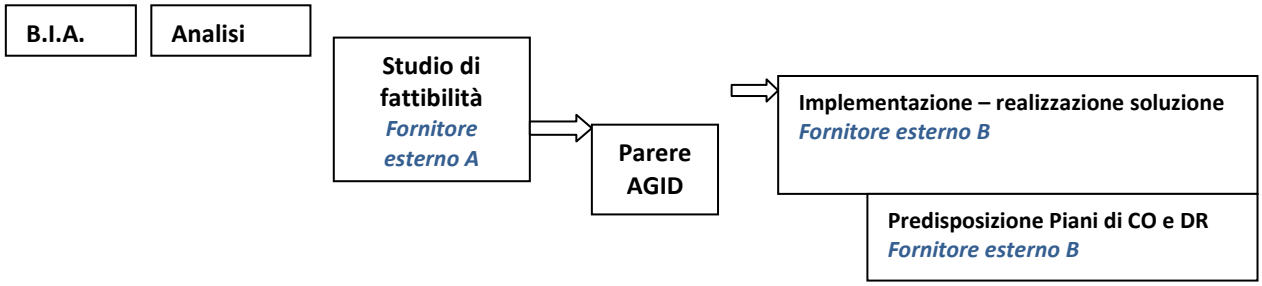


6.2.3 Ipotesi C: percorso di attuazione della soluzione di CO e DR affidato ai fornitori

In detta ipotesi di massima possono essere richiesti servizi per la progettazione ma anche per la realizzazione e della soluzione di CO/DR realizzata.

Anche in questo caso, il processo prenderà le mosse dalla preliminare ricognizione del contesto tecnico che connota il Sistema Informativo primario per il quale deve essere progettata la soluzione.

Ipotesi C: l'intero processo è oggetto di acquisizione



6.2.4 Outsourcing dei servizi ICT: avvertenze

Anche alla luce dell'esperienza condotta nelle fasi di istruttoria delle richieste di parere, si ritiene opportuno segnalare alle Amministrazioni che anche i servizi necessari al proprio funzionamento gestiti tramite outsourcer, devono disporre di soluzioni di CO/DR conformi ai requisiti che l'Amministrazione ha individuato e definito nella fase della BIA e nella conduzione del percorso di autovalutazione per gli altri servizi.

Si è infatti riscontrato che alcune Amministrazione hanno ritenuto "In ambito" e sottoposti al percorso di autovalutazione e alla copertura dei piani di CO/DR solo i servizi ICT gestiti internamente, ritenendo che i servizi gestiti in outsourcing non dovessero essere oggetto sia dello Studio di fattibilità tecnica, sia dei Piani di CO/DR perché affidati all'outsourcer.
Alla luce dell'art. 50bis si sottolinea l'importanza di ricomprendere nei Piani di CO/DR sia i servizi ICT c.d., gestiti internamente, che eventuali servizi ICT affidati all'outsourcer; è fondamentale per l'Amministrazione garantire, fermo il rispetto della normativa in tema di appalti, che tutti i servizi ICT essenziali all'attività istituzionale siano garantiti da adeguate soluzioni per la salvaguardia dei dati e delle applicazioni, definendo opportunamente le modalità, i termini e i requisiti.

6.2.5 La realizzazione di soluzioni di continuità operativa

Nella realizzazione delle soluzioni di CO/DR le Amministrazioni, in linea di massima, possono garantirsi:

1. la sola **salvaguardia dei dati e delle applicazioni**: questa soluzione è da ricercare quando un'Amministrazione stima che non sia necessaria una disponibilità più o meno immediata per l'accesso ai dati. Può essere il caso di un servizio di conservazione di dati storici che non contemplino una frequenza di accesso periodica (per esempio, dati relativi a pratiche di oltre quindici-venti anni, che possono essere consultate solo eccezionalmente o molto raramente); naturalmente, anche la sola salvaguardia dei dati e delle applicazioni può richiedere che questa avvenga minimizzando i disallineamenti tra dati primari e dati remoti (RPO basso);
2. **l'accesso a contratti standard di Disaster Recovery**: si tratta delle offerte di servizi di DR che i fornitori di questi servizi mettono a disposizione di tipologie di utenza generiche (imprese, finanza, assicurazioni); in genere, consistono nella possibilità di accedere a periodi temporalmente limitati di disponibilità di sistemi (60-90 giorni) e, anche in questo caso, possono consistere nella sola salvaguardia dei dati e delle applicazioni;
3. **soluzioni personalizzate**: se le esigenze di continuità dei servizi IT di un'Amministrazione e la numerosità e/o la criticità delle applicazioni e delle utenze sono particolarmente elevate, oppure esistono particolari requisiti, quali l'esigenza di isolare le infrastrutture di DR da quelle condivise da altre utenze, un'Amministrazione deve predisporsi a ricercare soluzioni che siano sviluppate per le proprie specifiche esigenze. Si tratta di soluzioni che solo Amministrazioni molto grandi o che svolgano servizi di particolare delicatezza dovrebbero ricercare.
4. **il mutuo soccorso**: il mutuo soccorso, che può anche realizzarsi per la semplice salvaguardia dei dati e delle applicazioni, è una via perseguibile solo quando due o più Amministrazioni sono in presenza di due fattori precisi:
    a) la disponibilità di risorse logistiche e IT che siano in esubero rispetto ai bisogni di ciascuna;
    b) la volontà di condividere queste risorse con altre Amministrazioni.

   Si tratta di una soluzione che rappresenta al meglio lo spirito di collaborazione all'interno della PA, ma che comunque implica molta attenzione, non solo al quadro normativo di riferimento (con

particolare riguardo alla conformità con quanto previsto dal D.lgs. 196/03 e s.m.i. ("Codice in materia di protezione dei dati personali") relativamente alle misure tecniche ed organizzative da adottare per la protezione dei dati personali trattati dall'Amministrazione) e agli aspetti procedurali (per esempio: la regolamentazione dell'accesso, potenzialmente prolungato, a locali di personale esterno, non solo dell'Amministrazione "mutuata", ma anche di fornitori di questa; le potenziali differenze di esigenze operative, quali orari differenti di disponibilità dei servizi, che rendano necessario, sempre all'Amministrazione "mutuata", la presenza di personale in orari di chiusura dell'Amministrazione "mutuante").
Per maggiori dettagli si rinvia a quanto indicato nell'appendice D4 al presente documento.

6.3 Richiami alla principale normativa di riferimento per le procedure di acquisizione di beni e servizi

Il conferimento da parte di una PA, a un apposito soggetto, dell'incarico di erogare i servizi e fornire i beni necessari ad assicurare all'Amministrazione medesima la continuità operativa, dovrà essere preceduto dallo svolgimento della procedura di selezione del contraente.
La principale normativa comunitaria e nazionale di riferimento per l'attuazione di soluzione di continuità operativa e di DR è la seguente:

- Direttiva 31 marzo 2004, n. 2004/18/CE: "Direttiva del Parlamento europeo e del Consiglio relativa al coordinamento delle procedure di aggiudicazione degli appalti pubblici di lavori, di forniture e di servizi";
- D. Lgs. 12 aprile 2006, n. 163 e s.m.i.: "Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE" e il relativo Regolamento di attuazione ed esecuzione il DPR 702/2010;
- DPCM 6 agosto 1997, n. 452 (GU. 30 dicembre 1997, n. 302): "Regolamento recante approvazione del capitolato di cui all'articolo 12, c. 1, del D.lgs. 12 febbraio 1993, n. 39, relativo alla locazione e all'acquisto di apparecchiature informatiche, nonché alla licenza d'uso dei programmi";
- L. 12 luglio 2011, n. 106 di "Conversione in L., con modificazioni, del decreto Legge. 13 maggio 2011, n. 70", concernente "Semestre Europeo. Prime disposizioni urgenti per l'economia".
- D.lgs. 196/2003 e s.m.i. (così come modificato da ultimo alla luce del D.lgs. 28 maggio 2012, n. 69), che contiene "il Codice in materia di protezione dei dati personali".
- L. 135 del 7 agosto 2012 di "Conversione in L. con modificazioni del decreto L. 6 luglio 2012, n. 95: Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini nonché misure di rafforzamento patrimoniale delle imprese del settore bancario";
- Anche in questa materia, appare utile ricordare le prescrizioni contenute nelle "Linee Guida per la qualità dei beni e dei servizi ICT nella PA" (Quaderno CNIPA 31/1-7).

Per la specifica necessità dell'acquisizione di beni e servizi per la Continuità Operativa, l'art. 50bis c. 4 del CAD impegna le Amministrazioni a definire piani di continuità operativa e di Disaster Recovery sulla base di appositi e dettagliati studi di fattibilità tecnica. Questa previsione normativa, conferma la previgente disciplina: anche qualora si debba addivenire all'adozione di soluzioni di CO/DR, rimane ferma la necessità di un'analisi costi-benefici per lo studio di fattibilità ex art. 50bis, nonché l'obbligo ex artt. 9 e 17, c. 2, D.lgs 12 febbraio 1993, n. 39 ed art. 3 del DPCM 6 agosto 1997, n. 452, che già richiedevano la redazione dello studio di fattibilità tecnico-economica per i contratti di grande rilievo.
Nella tabella seguente, riprendendo la tabella a pagina 52 che descrive gli elementi di massima dei Tier come definiti precedentemente e rimandando all'appendice al presente documento, per ulteriori suggerimenti e dettagli, si riepilogano in forma schematica per ciascun Tier, gli adempimenti e aspetti da verificare e che devono essere disciplinati sia nel contratto che regolerà le prestazioni richieste a un

fornitore esterno per la soluzione di DR sia nel caso di utilizzo di servizi RaaS (recovery as a service) presso provider esterni.

I LIVELLI DELLE SOLUZIONI *(TIER LG)*	IPOTESI DI MASSIMA DEGLI ADEMPIMENTI DA VERIFICARE (OLTRE RTO ED RPO) E DA DISCIPLINARE NEL CONTRATTO
Tier 1:	-Verifica periodica (es. con finestra di rilevazione mensile/trimestrale ecc.) e verifiche degli ambienti e dei supporti in modo più frequente: -Aderenza del sito ai requisiti richiesti -Rispetto tempi e modalita' di svolgimento del servizio di trasporto -Garanzia di corretta conservazione delle copie dati in luoghi adeguati e che consentano il recupero delle stesse copie ove necessiti.
Tier 2: .	-Verifica periodica (es. con finestra di rilevazione mensile/trimestrale) e verifiche degli ambienti e dei supporti in modo più frequente; -Aderenza del sito ai requisiti richiesti; -Rispetto tempi e modalita' di svolgimento del servizio di trasporto; -Garanzia di corretta conservazione delle copie dati in luoghi adeguati e che consentano il recupero delle stesse copie ove necessiti; -RPO:possibile solo verifica a campione "consistenza" dati sulle copie; -Disponibilità di storage e risorse elaborative nei tempi definiti in caso di disaster.
Tier 3:	Verifica periodica (es. con finestra di rilevazione mensile/trimestrale ecc.) e durante i test; -Disponibilità e rispondenza del sito ai requisiti richiesti; -Disponibilità del collegamento di rete; -Velocità di trasferimento dati; -Disponibilità storage; -Disponibilità risorse elaborative
Tier 4:	-Verifica periodica (es. con finestra di rilevazione mensile/trimestrale ecc.) e durante i test; -Disponibilità e rispondenza del sito ai requisiti richiesti; -Disponibilità del collegamento di rete; -Velocità di trasferimento dati; -disponibilità di storage -Disponibilità di risorse elaborative.
Tier 5:	-Verifica periodica (es. con finestra di rilevazione mensile/trimestrale ecc.) e durante i test; -Disponibilità e rispondenza del sito ai requisiti richiesti; -Disponibilità del collegamento di rete; -Velocità del trasferimento dei dati; -Disponibilità di storage -Disponibilità risorse elaborative.
Tier 6:	-Verifica periodica (es. con finestra di rilevazione mensile/trimestrale ecc.) e durante i test; -Disponibilità e rispondenza del sito ai requisiti richiesti; -Disponibilità del collegamento di rete; -Velocità del trasferimento dei dati; -Disponibilità di storage; -Disponibilità di risorse elaborative.

Ulteriori dettagli in merito alla normativa di riferimento sono riportati in Appendice al presente documento.

6.4 Le acquisizioni tramite Convenzioni, Accordi Quadro, MEPA e Contratti Quadro

Appare opportuno anche ricordare che per l'acquisto di beni e servizi, le Amministrazioni interessate a realizzare una soluzione di continuità operativa, devono anche tener conto dell'offerta presente sulle Convenzioni stipulate da Consip ai sensi dell'art. 26 della L. 488 del 23 dicembre 1999 e sul Mercato Elettronico della PA (www.acquistinretepa.it); le singole Amministrazioni, infatti, possono perfezionare ordinativi di fornitura, entro il massimale economico e i quantitativi previsti nei citati strumenti di acquisto.

Salvo restando quanto già detto nei precedenti paragrafi, la L. n. 191/09 del 23 dicembre 2009 (Finanziaria 2010, pubblicata in G.U. il 30 dicembre 2009 ed in vigore dal 1° gennaio 2010) attribuisce a

Consip la possibilità di stipulare anche Accordi Quadro di cui all'art. 59 del Codice De Lise: sia per consentire poi la definizione di appalti specifici fra le singole Amministrazioni e i fornitori aggiudicatari degli accordi quadro, che per addivenire, in sede di aggiudicazione degli appalti specifici, alla definizione, delle citate Convenzioni di cui all'art. 26 della citata L.. 488 del 23 dicembre 1999.
Le Amministrazioni interessate potranno poi, nell'ambito delle Convenzioni così definite, perfezionare i singoli ordinativi di fornitura.

6.4.1 Connettività e servizi SPC

Le soluzioni di Disaster Recovery possono prevedere una componente di rete per la connettività tra sito primario e sito alternativo. Si ricorda che nel caso di sito primario gestito da un fornitore, e non direttamente dall'Amministrazione, è necessario inserire come vincolo contrattuale al fornitore del sito primario l'obbligo di accettazione delle soluzioni di rete richieste dal Disaster Recovery, così come anche l'obbligo di accettare e mettere in opera, per quanto di competenza, tutte le attività sistemistiche occorrenti per la connessione di trasporto e tra i sistemi.

Per quanto attiene alla scelta della componente di rete, devono essere considerati i seguenti passi:

- innanzi tutto, deve essere verificato se esistano nel listino SPC servizi che siano coerenti con i requisiti della componente di rete;
- nel caso in cui non siano reperibili nel listino SPC servizi ritenuti corrispondenti ai requisiti, sia per ragioni inerenti le caratteristiche della rete (quale, a esempio, il tempo di ritardo di attraversamento della rete), sia per considerazioni di maggiore convenienza economica se utilizzate altre disponibilità di mercato, la componente di rete va ricercata seguendo le normali procedure che regolano gli appalti pubblici.

6.5 Cenni agli strumenti e clausole da adottare per soluzioni cloud che implichino il trasferimento dei dati (rinvio alla normativa comunitaria e ai provvedimenti del Garante per la protezione dei dati personali)

Con il termine *cloud computing* si intende la disponibilità, in modalità *on demand*, di risorse informatiche (applicazioni, DB, file service…) viste come servizi tramite l'accesso ad una rete di computer la cui reale dislocazione sul territorio di norma può essere sconosciuta all'utente, il quale,quindi, può operare ignorando la reale natura, struttura e collocazione delle risorse impiegate, utilizzandole in modalità *"service"* e accedendo ovi tramite Internet (*Public cloud*) o tramite intranet private (*Private cloud*).
I due modelli di cloud (*private, public*) possono coesistere in quello che viene definito *Hybrid cloud*:
un esempio è l'utilizzo di un servizio di private cloud per la maggior parte delle applicazioni critiche e per quelle che gestiscono dati sensibili e un public cloud per il resto delle applicazioni. La parte public cloud potrebbe anche essere utilizzata solamente per ottenere on-demand risorse elaborative o di storage aggiuntive al fine di gestire i picchi di carico delle applicazioni.
Sostanzialmente, l'approccio ibrido consente di sfruttare la scalabilità e convenienza che offre un ambiente di cloud computing pubblico senza esporre a vulnerabilità le applicazioni critiche e i dati sensibili.
Altra tipologia è sicuramente quella definita "*Public cloud"* che prevede l'utilizzo di servizi, forniti da soggetti terzi secondo uno schema riconducibile alla categoria dell'outsourcing, garantiti da infrastrutture la cui reale dislocazione sul territorio, di norma, è sconosciuta all'utente.

Quindi, utilizzando il *Public cloud*, tutti i dati, o anche solo parte di essi, può transitare e/o risiedere al di fuori del territorio nazionale o addirittura dell'UE, spesso in più luoghi fisici non conosciuti né conoscibili da parte del titolare dei dati.
Se da un lato l'aspetto delle caratteristiche del servizio può essere gestito agevolmente mediante l'adozione di opportune clausole contrattuali, più complesse appaiono le problematiche derivanti dall'applicazione della normativa sulla protezione dei dati personali.

Affidare all'esterno della Amministrazione la gestione di determinati servizi implica, in generale, il trattamento di dati da parte del fornitore del servizio che può risiedere in stati al di fuori del territorio nazionale in stati soggetti a giurisdizioni diverse.
Questo risulta ancora più importante nel caso di fornitori servizi *cloud*, poiché alcuni di questi non comunicano l'esatta locazione geografica dei dati gestiti in quanto, per le caratteristiche stesse della tecnologia in questione, gli stessi dati possono essere continuamente movimentati su locazioni diverse (ad es., perché un sito ha un carico operazionale molto alto e quindi parte di questo carico deve essere trasferito).

Il Codice in materia di protezione dei dati personali (D.lgs. 196/2003 e s.m.i.), oltre a regolare i diritti dell'interessato, prevede gli obblighi di acquisizione del consenso dell'interessato e di informativa e disciplina: i ruoli e compiti dei soggetti che effettuano il trattamento (il titolare, il responsabile, gli incaricati); gli adempimenti e le misure per garantire la corretta gestione e trattamento dei dati (soprattutto quelli sensibili); la sicurezza dei dati e dei sistemi (in particolare nel titolo VII della parte I del citato D.lgs. 196/2003 e s.m.i. che regola il "Trasferimento dei dati all'estero").
Per maggiori dettagli e per un richiamo più esteso alla normativa citata, si rimanda all'appendice al presente documento.

Nella scelta di soluzioni che comportano il trasferimento dei dati, come avviene attraverso le soluzioni *cloud*, è necessario tener presente anche quanto indicato nella Decisione 2010/87/UE del 5 febbraio 2010 (relativa alle clausole contrattuali tipo per il trasferimento dei dati personali e incaricati del trattamento stabiliti in paesi terzi, a norma della Direttiva 95/46/CE del Parlamento europeo e del Consiglio) a seguito della quale il Garante per la protezione dei dati personali ha emanato il 27 maggio 2010 l'autorizzazione al trasferimento dei dati personali del territorio dello Stato verso Paesi non appartenenti all'Unione Europea, precisando gli aspetti e i requisiti minimi da rispettare e purché effettuati in conformità alle clausole contrattuali tipo riportati in allegato alla richiamata Decisione.

Nel caso in cui già a livello di sistema informativo primario la soluzione preveda un'architettura di tipo cloud è necessario indicare con precisione i requisiti e i vincoli che sono stati imposti al provider e il dettaglio delle modalità di ripristino dei dati in ottica di Disaster Recovery valutando, quindi, opzioni che garantiscano non solo il salvataggio remoto (backup) ma anche la possibilità di ripristino degli stessi, entro termini definiti, con adeguati livelli di servizio.
E' in ogni caso necessario che il fornitore sia tenuto a indicare, con apposita dichiarazione resa in sede contrattuale, l'esatta localizzazione, o le esatte localizzazioni dei dati gestiti.
Risulta evidente quanto sia necessario identificare e indicare con precisione i requisiti e i vincoli contrattuali a cui deve sottostare il fornitore di servizi, sopratutto considerando che una notevole mole di dati può trovarsi a transitare e/o risiedere all'estero, spesso fuori dall'Unione Europea.
L'Unione Europea nella richiamata decisione ha stabilito che, in considerazione del progresso tecnologico, non è attuabile l'idea di limitare la circolazione dei dati ai soli paesi membri ma che, comunque, il loro trasferimento in paesi al di fuori dell'Unione debba avvenire garantendo il medesimo livello di protezione che gli stessi hanno in patria. Preso atto che le legislazioni, sopratutto

relativamente alla protezione dei dati, possono essere molto diverse nei paesi terzi e non garantire livelli di protezione adeguate, si rende quindi necessario agire contrattualmente, applicando delle clausole specifiche elaborate dalla Commissione Europea, nei contratti di fornitura del servizio.

Le nuove clausole, effettive dal 15 maggio 2010, trasferiscono parte delle responsabilità sul trattamento dati a chi effettivamente processa i dati. Considerato che l'attività di outsourcing può essere subappaltata anche più volte, nell'ambito del medesimo servizio, deve comunque essere garantita chiarezza su chi sia il responsabile per la sicurezza dei dati.
L'importatore (il soggetto che riceve inizialmente i dati nell'ambito del servizio offerto) è sempre l'unico responsabile per la loro sicurezza anche in caso di subappalto a terzi che comunque:

- deve essere autorizzato per iscritto dall'esportatore (ovvero chi invia i dati fuori dalla UE);
- deve prevedere, per il subappaltatore, l'applicazione delle stesse clausole contrattuali che è tenuto a rispettare l'importatore;
- prevede che l'importatore invii una copia del contratto, siglato con il subappaltatore, all'esportatore.

Questi vincoli garantiscono che l'esportatore sia sempre a conoscenza dei contratti di subappalto in corso, relativamente ai dati di sua competenza e gli impongono anche di conservare una copia di tutti i contratti di subappalto e delle autorizzazioni a procedere inviate all'importatore che dovranno essere presentati all'autorità garante in caso di richiesta.

L'utilizzo di servizi in modalità cloud, come evidenziato dal documento "Raccomandazioni e proposte sull'utilizzo del cloud computing nella PA", pubblicato da Digitpa il 28 giugno 2012 (e disponibile sul sito dell'Agenzia per l'Italia digitale) può permettere non solo di ridurre, potenzialmente, i costi di infrastruttura, ma anche di poter far fronte a particolari incrementi dell'attività (es.: necessità di maggiore capacità computazionale; necessità di maggiore storage; necessità di maggiore traffico internet; etc.), anche limitati nel tempo, semplicemente chiedendo un upgrade del servizio fornito.
Si ritiene altresì opportuno in materia segnalare l'importanza di consultare anche il documento "Cloud computing: indicazioni per l'utilizzo consapevole dei servizi", allegato alla redazione annuale 2010 del Garante e reperibile sul sito web del Garante all'indirizzo http://www.gpdp.it/garante/documenti?ID=18199333", nonché la miniguida "Cloud Computing. – Proteggere i dati per non cadere dalle nuvole", pubblicata dal Garante nel maggio del 2012.

Dal punto di vista operativo lo schema applicabile potrà essere quello dei punti 6.2.2. o 6.2.3.
Gli elementi di massima costituenti una soluzione Cloud di DR, previa attenta verifica, come detto nei documenti citati, sia delle caratteristiche tecniche dei sistemi e delle applicazioni, sia del contesto di riferimento del sistema informativo interessato, potranno essere i seguenti:

- server virtuali;
- sw di data replication;
- spazio disco;
- servizi professionali di:
    - installazione di base per la prima messa in opera;
    - configurazione, collaudo e messa in opera;
    - supporto per le prove di Disaster Recovery;
    - gestione server virtuali e storage sul sito di DR;
    - gestione appliance su sito Cliente e su sito di DR;
- infrastruttura di rete IP (Router IP e bandwidth della linea) per il collegamento tramite WAN tra i siti sorgente del Cliente finale ed il Cloud Provider;
- ambiente di backup.

Contrattualmente, per ciascuno degli elementi di massima e delle componenti schematicamente richiamate, dovrà essere inserita la relativa disciplina, per assicurare il rispetto dei requisiti definiti dall'Amministrazione e la possibilità di verificare la messa a disposizione di quanto richiesto.
Il PCO può essere opzionalmente prodotto dal Cloud Provider in collaborazione con il fornitore dello Studio di Fattibilità e con l'Amministrazione.

In linea generale e anche con particolare riferimento ai modelli "Cloud", occorrerà anche prevedere che il Titolare del trattamento, oltre a ricorrere a Fornitori che garantiscano il rispetto di tutte le disposizioni in materia di protezione dei dati personali, debba affidare i dati a quei Fornitori che assicurino di:

- adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati dei clienti da parte degli addetti del Fornitore, quali che siano la loro qualifica, le loro competenze e gli ambiti di operatività e le finalità del trattamento;
- adottare protocolli di comunicazione sicuri che prevedano dei meccanismi che impediscano violazioni della sicurezza dei dati scambiati, come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi, e per garantire più in generale la sicurezza dei sistemi, evitando di esporli a vulnerabilità e a rischi di intrusione;
- garantire che i dati siano protetti contro il rischio di intrusione mediante idonei strumenti di protezione perimetrale a salvaguardia delle reti di comunicazione e delle risorse di memorizzazione ed elaborazione impiegate nei trattamenti;
- garantire l'isolamento logico dei dati dei clienti differenti ospitati sulle medesime infrastrutture, adottando adeguate misure tecnologiche, al fine di evitare che eventuali problemi in una comunità possano ripercuotersi su altre comunità e l'accesso di dati da parte di soggetti non autorizzati;
- in caso di trattamento di dati sensibili o giudiziari, ricorrere ai Fornitori che garantiscano di proteggere tali tipologie di dati con tecniche crittografiche e in particolare contro rischi di acquisizione fortuita o di alterazione accidentale;
- garantire la sicurezza fisica: il Titolare dovrebbe avvalersi di Fornitori di servizi che adottino specifiche misure di sicurezza fisica per garantire un adeguato livello di protezione dei sistemi che trattano i dati.

Oltre alle misure di carattere tecnologico, nelle norme **contrattuali** tra Titolare e Fornitore dei servizi cloud dovrebbe essere esplicitata almeno:

- la possibilità di svolgere attività di audit da parte dell'Amministrazione;
- la dichiarazione di compliance da parte del Fornitore alle misure di sicurezza prescritte;
- la definizione da parte del Fornitore della politica di gestione dei dati, con riferimento particolare alle sedi in cui i dati saranno conservati, alle responsabilità ed ai diritti di accesso agli stessi in relazione alla classificazione dei dati e dei supporti di conservazione;
- la possibilità di verificare periodicamente che siano effettivamente garantiti i requisiti e le misure richieste dall'Amministrazione.

7 CONTINUITÀ OPERATIVA E DISASTER RECOVERY DELLE INFRASTRUTTURE CRITICHE

Il compito affidato dal CAD a DigitPA e ora all'Agenzia per l'Italia Digitale di provvedere alla redazione delle Linee Guida sulla Continuità Operativa (CO) ed il Disaster Recovery nella Pubblica Amministrazione, rappresenta anche l'occasione per avviare all'interno della PA stessa una prima necessaria riflessione sulla protezione delle infrastrutture critiche, tematica oggetto di recenti interventi normativi e sempre più al centro dell'attenzione in tutti i paesi industrializzati nella definizione delle politiche di difesa nazionale.
Se la CO, infatti, rappresenta parte integrante delle politiche di sicurezza di un'organizzazione, la stessa assume maggiore rilevanza laddove quella organizzazione rivesta un ruolo strategico per la nazione o sia titolare di processi e/o infrastrutture necessarie a garantire la sicurezza del sistema paese.
Per tali ragioni è avvertita la necessità di individuare in DigitPA, ora nell'Agenzia per l'Italia Digitale, l'ente in grado di svolgere il ruolo di sensibilizzazione, stimolo, aggregazione e coordinamento delle iniziative in questa materia per tutto il settore pubblico, interagendo direttamente con le strutture della Presidenza del Consiglio impegnate a disegnare le strategie nazionali di protezione delle infrastrutture critiche.
Con il recente intervento del legislatore nazionale (D.lgs 61/2011) è stata recepita nel nostro ordinamento la Direttiva europea 114/2008 che regolamenta le modalità di identificazione delle infrastrutture critiche europee (ICE) ed avviato, anche in Italia, quel percorso necessario per allinearsi agli altri paesi dell'Unione e per garantire il coordinamento delle iniziative di protezione nelle eventualità di eventi che impattino su IC ubicate in almeno due paesi dell'UE.
Il citato provvedimento, inoltre, nel recepire la definizione adottata a livello europeo di *infrastruttura*[4] e di *infrastruttura critica*[5], consente di avviare una strategia nazionale di attuazione di politiche volte ad elevare il livello di sicurezza e di affidabilità di tutte le infrastrutture critiche del Paese.

La PA nel suo complesso e singoli elementi o sistemi di alcune amministrazioni non saranno estranei a questo processo di messa in sicurezza: questo breve capitolo, pertanto, ha come obiettivo quello di presentare la tematica nella sua generalità nell'attesa che vengano emanate ulteriori direttive che trattino il tema delle IC a livello nazionale.
Una volta che tali provvedimenti normativi saranno promulgati, la PA italiana dovrà assumere consapevolezza del proprio ruolo nell'ambito del processo di identificazione delle ICN, anche in relazione alle modalità di protezione che saranno disciplinate a livello nazionale.

Si pensi, per esempio, al mantenimento in sicurezza di tutti quei sistemi ICT di cui la PA è a vario titolo responsabile e che sono necessari - direttamente o indirettamente - a funzioni vitali della società: banche dati erariali e catastali, servizi di anagrafe, banche dati per i centri trasfusionali, servizi elettorali, basi dati di interesse nazionale previste dall'art. 60 del CAD, ecc.

[4] Un'infrastruttura che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico 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

5 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.

7.1 La protezione delle IC in Europa

Il Consiglio Europeo del giugno 2004 ha chiesto la preparazione di una strategia globale per la protezione delle Infrastrutture Critiche ed il 20 ottobre dello stesso anno la Commissione ha adottato una comunicazione relativa alla protezione delle Infrastrutture Critiche nella lotta contro il terrorismo [EU1], che presenta una serie di proposte per incrementare la prevenzione, la preparazione e la risposta a livello europeo in caso di attentati terroristici che coinvolgono le Infrastrutture Critiche.
Nel dicembre 2004 il Consiglio ha approvato, nelle sue conclusioni sulla prevenzione, la preparazione e la risposta in caso di attentati terroristici, la proposta della Commissione di istituire un programma europeo per la protezione delle Infrastrutture Critiche (European Programme for Critical Infrastructure Protection, EPCIP), che comprende varie iniziative, finalizzate specificamente a migliorare la protezione delle Infrastrutture Critiche.

In particolare, tra gli aspetti caratterizzanti il programma EPCIP, vanno ricordati:
- la realizzazione di una rete informativa per la protezione delle Infrastrutture Critiche (*Critical Infrastructure Warning Information Network, CIWIN*);
- l'erogazione di finanziamenti per la realizzazione di progetti sulle IC;
- il varo di una Direttiva riguardante le Infrastrutture Critiche europee.

Ritornando alle attività in UE, nel novembre 2005 la Commissione ha adottato un Libro Verde [EU2] che raccoglie indicazioni sulle diverse alternative strategiche possibili in materia di CIP.
Nelle conclusioni relative alla protezione delle Infrastrutture Critiche, il Consiglio "Giustizia e affari interni" (GAI) del dicembre 2005 ha invitato la Commissione a presentare una proposta di programma europeo per la protezione delle Infrastrutture Critiche.
La Comunicazione della Commissione ST16932 [EU3] presenta i principi, le procedure e gli strumenti proposti per attuare l'EPCIP. Tale attuazione sarà completata, se del caso, da specifiche comunicazioni settoriali relative all'approccio della Commissione in particolari settori di Infrastrutture Critiche.

La Direttiva [EU4], approvata nel dicembre 2008, espone le misure previste dalla Commissione ai fini dell'individuazione e della designazione delle Infrastrutture Critiche Europee e della valutazione della necessità di migliorarne la protezione.
Partendo dalla considerazione che nell'Unione Europea vi sono varie infrastrutture il cui malfunzionamento o distruzione può avere un impatto su vari Stati Membri, la Direttiva fornisce le seguenti definizioni:
- "*Infrastruttura Critica" (IC):* quei beni, sistemi o parti di essi collocati negli Stati Membri della UE, che sono essenziali per il mantenimento delle funzioni sociali vitali, della salute, della sicurezza (*security* e *safety*), del benessere economico e sociale della popolazione, e la cui distruzione o il cui malfunzionamento avrebbe come diretta conseguenza un impatto significativo su uno Stato Membro, come risultato del mancato svolgimento di queste funzioni (*loss of service*);
- "*Infrastruttura Critica Europea" (ICE):* infrastruttura critica collocata negli Stati Membri della EU e la cui distruzione o il cui malfunzionamento avrebbe come diretta conseguenza un impatto significativo su almeno due Stati Membri dell'EU. La significatività dell'impatto deve essere stabilita in termini di criteri trasversali (*cross-cutting*). Questo comprende gli effetti derivanti da dipendenze intersettoriali su altri tipi di infrastrutture.

Si osservi che la definizione di Infrastruttura Critica data nella Direttiva si concentra unicamente sui due aspetti: il mancato servizio (*loss of service*) e l'impatto che il mancato servizio induce.
La Direttiva 114/08 CE delinea un approccio *all hazard*, prendendo in considerazione l'aspetto della valutazione dell'impatto in modo indipendente dalla minaccia che ha indotto il disservizio: in questo senso, quindi, tutti i tipi di minacce, da quelle naturali, a quelle legate alle attività antropiche, dagli incidenti occasionali agli attacchi terroristici deliberati, sono potenzialmente considerabili come causa del disservizio dell'Infrastruttura Critica sotto osservazione.

Uno dei temi fondamentali affrontati dalla Direttiva è quello della definizione di un approccio comune per l'individuazione delle Infrastrutture Critiche Europee e per la loro protezione.

Poiché vari settori dispongono di un'esperienza, di una competenza e di requisiti particolari in materia di protezione delle Infrastrutture Critiche, la Direttiva è concepita su base settoriale ed è attuata secondo un elenco stabilito di settori di IC. Allo stato attuale, i due settori individuati dalla Direttiva, a cui si stanno applicando le procedure per l'individuazione delle Infrastrutture Critiche Europee, sono quelli dell'Energia e dei Trasporti, e precisamente:

Settore
ENERGIA
Sottosettori

- Elettricità, comprendente: infrastrutture e impianti per la produzione e la trasmissione di energia elettrica e per la fornitura di elettricità;
- Petrolio, comprendente: produzione, raffinazione, trattamento, stoccaggio e trasporto di petrolio attraverso oleodotti;
- Gas, comprendente: produzione, raffinazione, trattamento, stoccaggio e trasporto di gas attraverso oleodotti e terminali GNL;

Settore
TRASPORTI
Sottosettori

- Trasporto stradale; Trasporto ferroviario; Trasporto aereo;
- Vie di navigazione interna;
- Trasporto oceanico, trasporto marittimo a corto raggio e porti.

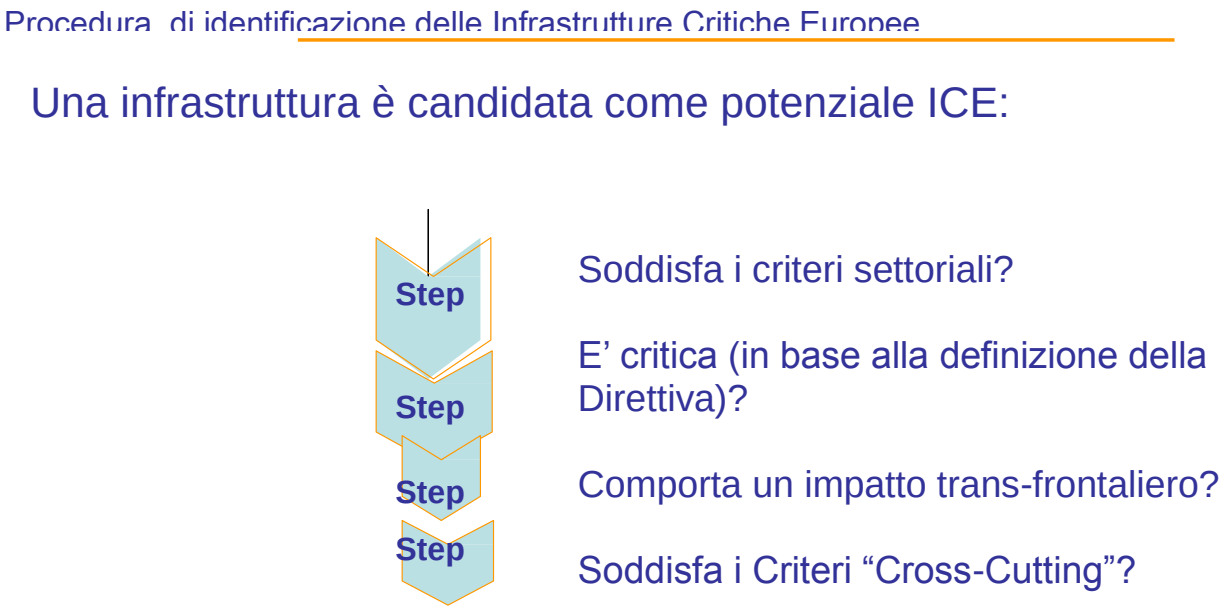
La Direttiva riconosce la necessità di estendere in futuro la lista dei settori critici, ed assegna la priorità al settore della *Information and Communication Technology (ICT*) già dalla prima revisione della direttiva stessa. Infatti, l'ICT costituisce oramai un servizio trasversale rispetto ai vari settori, capace, se in crisi, di avviare un effetto domino immediato e dagli impatti devastanti.

Vale inoltre la pena ricordare che nel programma EPCIP sono considerati vari ulteriori settori (come si evince dalla tabella seguente), che non sono stati tuttavia inseriti nella versione attuale della Direttiva al fine di giungere in tempi brevi ad una versione di compromesso condivisa tra tutti gli Stati Membri ed effettuare un primo test sulla applicazione della direttiva stessa con un numero ridotto di settori. Nella revisione della direttiva, prevista a partire dal 2012, verranno inseriti, a partire dall'ICT come già detto, anche gli altri settori mancanti, nell'ordine che verrà concordato tra gli Stati membri.

Elenco dei settori del programma EPCIP

UE esteso
Energia
Trasporti
Tecnologie dell'informazione e della comunicazione (ICT)
Acqua
Alimenti
Salute
Finanze
Industria chimica
Industria nucleare
Spazio
Ricerca

La Direttiva prevede l'applicazione di una procedura in quattro passi affinché un'infrastruttura sia designata ICE (o l'equivalente acronimo anglosassone ECI: *European Critical Infrastructure*); tale procedura è illustrata nella figura seguente.



- Step 1: facendo riferimento ai settori definiti nella precedente tabella, il primo passo richiede agli Stati Membri di verificare se le infrastrutture potenzialmente critiche soddisfino i criteri settoriali relativi. La Direttiva stabilisce che i criteri settoriali vengono definiti con il contributo e il consenso delle parti coinvolte prendendo atto del fatto che spesso nell'ambito dei settori individuati come critici esistono già criteri consolidati per l'analisi dei rischi e l'individuazione delle criticità. L'applicazione del primo passo consente di effettuare una prima cernita all'interno di ogni settore.

- Step 2: ogni Stato Membro dovrà verificare se le infrastrutture selezionate nel primo passo soddisfino la definizione di infrastruttura critica riportata in questo paragrafo.
- Step 3: ogni Stato Membro dovrà verificare se le infrastrutture selezionate nel secondo passo soddisfino la definizione di trans-nazionalità riportata in questo paragrafo, vale a dire, se un potenziale malfunzionamento o distruzione dell'infrastruttura può avere un impatto su almeno due Stati Membri.
- Step 4: occorre quindi effettuare un "livellamento" delle infrastrutture individuate, per garantire che vengano designate come ICE tutte e sole quelle infrastrutture che soddisfano un criterio comune e omogeneo di criticità. A tal fine, devono essere applicati criteri intersettoriali (*cross-cutting*) che tengono in considerazione i seguenti aspetti: conseguenze sulla salute dei cittadini, conseguenze economiche, conseguenze sull'opinione pubblica.

Come illustrato nella figura precedente, nel caso in cui un'infrastruttura superi i quattro passi della procedura, segue una fase di natura politica, in cui spetta comunque allo Stato Membro nel cui territorio risiede l'infrastruttura la decisione finale di designare tale infrastruttura come ICE.

Gli adempimenti imposti dalla Direttiva

Come si è detto, la Direttiva stabilisce una serie di procedure e azioni per l'individuazione e la protezione delle Infrastrutture Critiche Europee. In particolare, l'attuazione della Direttiva comporta una serie di adempimenti per i Paesi Membri, riassunti nel seguito.

Individuazione delle ICE

La Direttiva prevede l'applicazione di una procedura in vari passi affinché un'infrastruttura sia
riconosciuta come ICE. In particolare, nel quadro della Direttiva sono indicati i criteri settoriali e criteri inter-settoriali per selezionare quelle infrastrutture la cui rilevanza a livello comunitario è tale da ritenerle di interesse europeo. Spetta infine ad ogni Stato Membro la designazione finale dell'infrastruttura come ICE, mediante una comunicazione alla Commissione. Come già detto, allo stato attuale la Direttiva indica come settori prioritari, a cui deve essere applicata da subito la procedura per l'individuazione delle Infrastrutture Critiche Europee, quelli dell'Energia e dei Trasporti.

Punto di Contatto

Ogni Stato Membro interagirà con gli altri Stati Membri e con la Commissione mediante un organismo nazionale competente per la protezione delle Infrastrutture Critiche. Inoltre, per garantire il coordinamento delle attività, ciascuno Stato Membro ha nominato un Punto di Contatto unico.

Valutazione delle minacce e dei rischi

Agli Stati Membri è richiesto di svolgere una valutazione dei rischi, delle minacce e delle vulnerabilità con cadenza regolare; in particolare, devono essere analizzati i sottosettori nei quali sono state designate delle ICE.

Piani di Sicurezza dell'Operatore

Ogni proprietario/operatore di Infrastruttura designata come ICE dovrà dotarsi di un Piano di Sicurezza dell'Operatore (PSO). La Direttiva fornisce un'indicazione dei contenuti minimi che dovranno essere trattati nel Piano; in particolare, il PSO deve identificare i beni dell'infrastruttura critica e le soluzioni in atto o in corso di implementazione per la loro protezione.

Le procedure dovranno coprire almeno:

- l'identificazione dei beni critici;
- un'analisi dei rischi che comprenda le minacce, le vulnerabilità e l'impatto potenziale per ogni bene;
- l'identificazione, la selezione e la prioritarizzazione delle contromisure suddivise tra quelle permanenti e quelle attuabili gradualmente;

Funzionario di collegamento

Ogni proprietario/operatore di Infrastruttura designata come ICE dovrà nominare un funzionario di collegamento in materia di sicurezza che agisca come punto di contatto per le questioni di sicurezza fra l'ICE e l'organismo nazionale competente per la protezione delle Infrastrutture Critiche.

7.2 Cenni alle azioni in Italia

Il D.L. 27-7-2005 n. 144, convertito in legge, con modificazioni, dall'art. 1, L. 31/07/2005, n. 155, "Misure urgenti per il contrasto del terrorismo internazionale", all'art. 7-bis. Sicurezza telematica recita: "Ferme restando le competenze dei Servizi informativi e di sicurezza, di cui agli articoli 4 e 6 della legge 24 ottobre 1977, n. 801, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione *(Polizia Postale, nda)* assicura i servizi di protezione informatica delle *infrastrutture critiche informatizzat*e di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate. …".

Il Decreto del Ministro dell'Interno del 9 gennaio 2008 "Individuazione delle infrastrutture critiche informatiche di interesse nazionale" pubblicato nella GU n. 101 del 30-4-2008 recita:

"1. Ai sensi e per gli effetti dell'art. 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, sono da considerare infrastrutture critiche informatizzate di interesse nazionale i sistemi ed i servizi informatici di supporto alle funzioni istituzionali di: a) Ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute; b) Banca d'Italia ed autorità indipendenti; c) società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500.000 abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque; d) ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'interno, anche su proposta dei prefetti - autorità provinciali di pubblica sicurezza.

2. I collegamenti telematici necessari per assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di cui al comma 1 sono definiti sulla base dell'individuazione delle strutture medesime da parte delle istituzioni, amministrazioni, autorità, società, enti, persone giuridiche pubbliche o private di cui al medesimo comma 1, mediante apposite convenzioni ai sensi dell'art. 15 della legge 7 agosto 1990, n. 241 e dell'art. 39 della legge 16 gennaio 2003, n. 3, stipulate, per il Ministero dell'interno, dal Capo della polizia, direttore generale della pubblica sicurezza e, per le istituzioni ed altri soggetti interessati, dai competenti organi amministrativi di vertice."

Con tali provvedimenti si è avviata in Italia la trattazione giuridica del tema delle infrastrutture critiche, dapprima rafforzando, ad opera dei decreti su citati, la loro sicurezza informatica da atti criminali ed illegali.

Per quanto riguarda gli aspetti di pianificazione e coordinamento, l'Ufficio del Consigliere Militare del Presidente del Consiglio dei Ministri ha avviato dal 2006 il "Tavolo per la

Protezione delle Infrastrutture Critiche – Tavolo PIC" al quale hanno partecipato i Dicasteri e le Istituzioni interessati alla protezione delle Infrastrutture Critiche. Attraverso questo Tavolo sono state concordate a livello nazionale le posizioni e le proposte che hanno portato prima alla negoziazione e poi all'approvazione della Direttiva 114/08 CE.
Oggi il Tavolo PIC è stato assorbito dal Nucleo interministeriale situazione e pianificazione (NISP), ai sensi del decreto legislativo di recepimento della direttiva pubblicato su G.U. il 4 maggio 2011.
Su incarico del Tavolo PIC la Commissione Interministeriale Tecnica di Difesa Civile (CITDC) costituita ad ottobre 2001 dal Ministro dell'Interno per supportare l'organizzazione nazionale di gestione delle crisi, ha elaborato, in coordinamento con l'Ufficio del Consigliere Militare, le procedure per l'individuazione e designazione delle Infrastrutture critiche nazionali (ICN) che daranno luogo a una direttiva nazionale sulla individuazione delle ICN.

Come previsto dalla Legge comunitaria 2009, inoltre, è stato emanato il Decreto legislativo 11 aprile 011, n. 61 "Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione" pubblicato nella GU n. 102 del 4 maggio 2011.
Il Decreto Legislativo affida al Nucleo interministeriale situazione e pianificazione (NISP), istituito con decreto del Presidente del Consiglio dei Ministri 25 maggio 2010, le funzioni specificate nel D. Lgs.. n.61 per l'individuazione e la designazione delle ICE.
Per tali fini il NISP è integrato dai rappresentanti del Ministero dello sviluppo economico, per il settore energia, del Ministero delle infrastrutture e dei trasporti ed enti vigilati, per il settore trasporti.
Il Decreto Legislativo individua, ancora, una "struttura responsabile", cui sono affidate, per il supporto al NISP, le attività tecniche e scientifiche riguardanti l'individuazione delle ICE e per ogni altra attività connessa, nonché per i rapporti con la Commissione europea e con le analoghe strutture degli altri Stati membri dell'Unione europea. Tale struttura è stata identificata nella Segreteria per le infrastrutture critiche (SIC) già istituita presso l'Ufficio del Consigliere Militare della Presidenza del Consiglio dei Ministri con DPCM del 22 dicembre 2010.
La Segreteria cura il coordinamento interministeriale delle attività nazionali, anche in ambito internazionale, e delle attività tecniche e scientifiche per l'individuazione e la designazione delle infrastrutture critiche nazionali ed europee e concorre al coordinamento per la loro protezione.
I settori considerati nel citato D. Lgs n.61 ed i criteri introdotti sono gli stessi della direttiva 114/08: energia e trasporti.

I Criteri settoriali sono riportati nelle linee guida emesse dalla Commissione Europea in accompagnamento alla direttiva 114/08 e sono riservati; e le soglie vengono stabilite caso per caso dalla SIC con i Ministeri competenti a livello settoriale.

I Criteri Intersettoriali (*cross-cutting*) per verificare la significatività dell'impatto sono rappresentati da:

- le possibili vittime, in termini di numero di morti e di feriti;
- le possibili conseguenze economiche, in termini di perdite finanziarie, di deterioramento del bene o servizio e di effetti ambientali;
- le possibili conseguenze per la popolazione, in termini di fiducia nelle istituzioni, di sofferenze fisiche e di perturbazione della vita quotidiana, considerando anche la perdita di servizi essenziali.

Per la definizione delle Soglie, la SIC effettua discussioni bilaterali o multilaterali con gli altri Stati Membri coinvolti dalla IC sotto esame e preliminarmente, in tali discussioni, fissa, in accordo con gli altri Stati, limiti comuni dei criteri di valutazione intersettoriale.

Le definizioni di Infrastruttura, di infrastruttura critica e di settore, come riportate nel decreto 61/2011, sono:

a) 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;
b) infrastruttura critica (IC): infrastruttura, ubicata in uno Stato membro dell'Unione europea, 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 in quello Stato, a causa dell'impossibilità di mantenere tali funzioni;
c) settore: campo di attività omogenee, per materia, nel quale operano le infrastrutture, che può essere ulteriormente diviso in sotto-settori;
d) infrastruttura critica europea (ICE): infrastruttura critica ubicata negli Stati membri dell'UE il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. *La rilevanza di tale impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture.*

L'IC ha una connotazione spaziale (geografica) e si identifica grazie al suo ruolo nella creazione e mantenimento della qualità della vita del cittadino. Perciò l'obiettivo di protezione identificato dallo Stato nel D. Lgs 61/2011 è la qualità della vita del cittadino e la sua continuità ad un livello predefinito e identificabile come uno "standard" di benessere sociale. Tale benessere è costituito dalla disponibilità di servizi e prodotti fruibili dal cittadino stesso e descrivibili in modo univoco da parametri di qualità del servizio/prodotto e da indici numerici o qualitativi che indicano, per ciascun parametro, il suo valore atteso e la sua probabilità nel tempo e nello spazio. Identificare e designare IC significa identificare quelle strutture che hanno un impatto determinante, nel caso di assenza del loro servizio o prodotto, sulla qualità della vita del cittadino.
In questo contesto, quindi, l'identificazione di una particolare infrastruttura come IC avviene sulla base di una valutazione dell'impatto derivante da un malfunzionamento che colpisce quella particolare infrastruttura. L'impatto si valuta tenendo in conto tutti gli effetti provocati dal malfunzionamento anche su altre infrastrutture e in modo indipendente dalla effettiva causa che potrebbe aver dato luogo alla crisi/evento. L'entità dell'impatto, quindi, è attribuibile unicamente alla condizione di fuori servizio (totale o parziale) della infrastruttura stessa con la conseguente perdita o riduzione del servizio/prodotto da essa erogato in condizioni "normali".
L'effettiva possibilità di valutare l'impatto di un malfunzionamento impone la conoscenza e l'analisi delle dipendenze **dirette e indirette** (fisiche, logiche, geografiche, organizzative, cyber, ecc.) tra infrastrutture.
L'approccio definito dalla direttiva 114/08 CE e mutuato nel D.lgs. n. 61/2011 ha il vantaggio di prescindere dallo scenario specifico che ha condotto alla crisi, basando la valutazione della criticità unicamente sull'impatto causato dalla crisi sulla popolazione e non anche sulla valutazione delle minacce e delle vulnerabilità.
Solo in fase di analisi dei rischi, condotta dai singoli operatori delle infrastrutture identificate come critiche, verranno considerati gli aspetti relativi alle specifiche minacce e alle eventuali vulnerabilità esibite dall'infrastruttura.
Gli indicatori prescelti dall'Unione Europea per consentire la valutazione d'impatto e mutuati nella legislazione italiana, sono:

- numero di vittime (valutato in termini di numero potenziale di morti e feriti);
- danno economico (valutato in termini di entità delle perdite economiche e/o del deterioramento di prodotti o servizi);
- effetti sull'opinione pubblica (valutati in termini di impatto sulla fiducia dei cittadini, sofferenze fisiche e perturbazione della vita quotidiana).

A questo riguardo occorre osservare che, nel valutare gli indicatori sopra elencati, è necessario specificare se essi debbano essere riferiti alle sole conseguenze del mancato servizio che si verifica a seguito di un evento (effetti negativi esterni, *consequence impacts*), oppure se debbano comprendere anche gli effetti dell'evento stesso (effetti negativi intrinseci, *ground zero impacts*). Ad esempio, nel caso di un attacco terroristico che coinvolga una stazione ferroviaria, le conseguenze (in termini di vittime, danno economico e effetto sull'opinione pubblica) direttamente legate all'evento hanno un peso molto maggiore rispetto alle conseguenze strettamente riconducibili all'assenza del servizio (il collegamento ferroviario, in questo caso) su altre infrastrutture. Nella metodologia di analisi scelta dall'Unione Europea, si è seguita la prima opzione, ovvero quella di considerare solo le conseguenze legate al mancato servizio: ciò è riconducibile al fatto che le conseguenze dirette di un evento sono generalmente di rilevanza strettamente nazionale, mentre la Direttiva Europea si pone nell'ottica di valutare i danni che abbiano un rilievo trans-nazionale. Nell'ambito di un'analisi nazionale, viceversa, le conseguenze dirette dovrebbero essere debitamente tenute in conto.
A valle della identificazione e designazione come IC europea occorre effettuare una serie di attività atte a proteggere o a migliorare, se necessario, la protezione dell'IC stessa.
L'identificazione, infatti, sotto le premesse suddette, è finalizzata a dare alla infrastruttura un obiettivo di protezione in più (la continuità di una determinata qualità del servizio/prodotto reso/i al cittadino) rispetto a quelli che già aveva (o avrebbe dovuto) adottare sulla base delle priorità stabilite dal proprio management (che tipicamente coincidono con l'adempimento degli obblighi di legge, la continuità "del guadagno", il mantenimento del capitale, il mantenimento del know-how, l'immagine, ecc.). La continuità operativa e il Disaster Recovery assurgono dunque a strumenti basilari di robustezza, laddove necessaria, e resilienza (ottimizzata sugli obiettivi di continuità del servizio) dell'IC.
La valutazione d'impatto che conduce all'identificazione di una IC si basa sull'assunto che l'impatto stesso sia valutato sull'interezza del sistema Paese e non solo, come spesso avviene nei modelli di analisi delle IC, sulle attività inerenti i settori assiomaticamente definiti "critici", cioè con potenziali IC al loro interno. Occorre, quindi, costruire un modello "macro" di funzionamento della società, in grado di consentire la valutazione delle conseguenze che la mancanza di un determinato servizio o prodotto indurrebbe su tutto l'assetto sociale, economico, politico, ecc.
Una volta assodato che una data infrastruttura, pubblica o privata, è una IC, l'IC stessa viene di fatto invitata (attraverso l'obbligo di redazione del PSO, almeno) a effettuare una analisi dei rischi che ponga come obiettivo di protezione l'obiettivo/i prescelto da chi la ha designata. A valle dell'analisi dei rischi è opportuno redigere piani di emergenza ed effettuare esercitazioni e test per "formare" tutti gli attori coinvolti nelle attività di protezione e sicurezza.
Il personale è sicuramente tutto coinvolto, a vari livelli, da tali attività. Tuttavia, un piano di emergenza tiene conto, oltre che della realtà interna alla IC o alla singola sede della IC, anche della realtà esterna (dislocazione fisica e geografica della IC o della sede, realtà operanti nella medesima zona, possibilità di evacuazione o invacuazione della zona, quantità di persone che insistono sulla medesima zona, attrattività degli attori operanti in zona, viabilità della zona a pieno regime di spostamento di tutta la popolazione che, nelle varie ore del giorno, insiste sulla zona stessa, capacità di assorbimento di picchi da parte del trasporto pubblico di zona, ecc.).

Alle ICE designate vengono richiesti alcuni adempimenti e cioè, in particolare, la nomina di un funzionario di collegamento in materia di sicurezza che è anche funzionario alla sicurezza in materia di tutela delle informazioni classificate, la realizzazione di una analisi dei rischi e la redazione di un Piano della Sicurezza dell'Operatore.
L'Allegato B al D. Lgs. 61/2011, riporta i Requisiti minimi del piano di sicurezza dell'operatore (PSO) e cioè:

"*Il piano di sicurezza dell'operatore (PSO) identifica gli elementi che compongono l'infrastruttura critica, evidenziando per ognuno di essi le soluzioni di sicurezza esistenti, ovvero quelle che sono in via di applicazione. Il PSO comprende l'individuazione degli elementi più importanti dell'infrastruttura:*

1. *l'analisi dei rischi che, basata sui diversi tipi di minacce più rilevanti, individua la vulnerabilità degli elementi e le possibili conseguenze del mancato funzionamento di ciascun elemento sulla funzionalità dell'intera infrastruttura;*
2. *l'individuazione, la selezione e la priorità delle misure e procedure di sicurezza distinte in misure permanenti e misure ad applicazione graduata. Le misure permanenti sono quelle che si prestano ad essere utilizzate in modo continuativo e comprendono:*
   - *sistemi di protezione fisica (strumenti di rilevazione, controllo accessi, protezione elementi ed altre di prevenzione);*
   - *predisposizioni organizzative per allertamento comprese le procedure di gestione delle crisi;*
   - *sistemi di controllo e verifica;*
   - *sistemi di comunicazione;*
   - *addestramento ed accrescimento della consapevolezza del personale;*
   - *sistemi per la continuità del funzionamento dei supporti informatici.*
3. *Le misure ad applicazione graduata da attivare in relazione al livello di minacce o di rischi esistenti in un determinato periodo di tempo.*

Inoltre, si devono applicare anche, in quanto compatibili, le disposizioni di cui agli artt. 11, 12 e 20 del decreto legislativo 17 agosto 1999, n. 334."

La descrizione del PSO è volutamente generica per non entrare in dettagli che solo normative di settore possono definire con pienezza e precisione specifiche e adeguate alle esigenze di ciascun settore. Entrare in ulteriori dettagli a livello "generalistico" avrebbe potuto abbassare gli standard di protezione e sicurezza già adottati a livello settoriale dalle singole autorità competenti.

Si segnala che la legge n. 133/2012, innovando la legge n. 124/2007, attribuisce al Presidente del Consiglio dei ministri fra gli altri, sentito il Comitato interministeriale per la sicurezza della Repubblica, il compito di "*impartire al Dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza direttive per rafforzare le attivita' di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali*".

Si rimanda altresì a quanto indicato nel DPCM del 24 gennaio 2013 recante indirizzi per la protezione cybernetica e la sicurezza informatica nazionale, diretto ad accrescere le capacità del Paese di confrontarsi con le minacce alla sicurezza informatica anche sotto il profilo della protezione delle infrastrutture critiche. Il decreto pone le basi per un sistema organico, all'interno del quale, sotto la guida del Presidente del Consiglio, le varie istanze competenti potranno esercitare in sinergia le rispettive competenze.

7.3 Conclusioni: la sicurezza informatica, la continuità operativa, le infrastrutture critiche

Come anticipato, uno degli obiettivi di queste linee guida è quello di indicare le iniziative necessarie nella PA per realizzare la capacità di risposta ad eventi che impattano sul normale funzionamento dei propri uffici, sempre più dipendenti dalle tecnologie ICT e, pertanto, esposti ad un numero crescente di rischi.

L'applicazione di questo principio alla PA nel suo complesso ed alle singole amministrazioni comporta l'adozione di una serie di iniziative e di processi interni il cui obiettivo è quello di garantire sempre, il rispetto dell'art. 97 della Costituzione e l'attuazione del combinato disposto dei

principi generali e degli artt.17 co.1, lett.c (Strutture per l'organizzazione, l'innovazione e le tecnologie), 50-bis (Continuità operativa) e 51 (Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni) del CAD.
La realizzazione di quanto previsto dall'art. 50bis del CAD e, conseguentemente, la messa a regime di quanto proposto con le presenti Linee Guida, consentirà l'attuazione di un modello omogeneo di soluzioni di continuità operativa e Disaster Recovery per tutta la PA, centrale e territoriale; il risultato più apprezzabile di questo processo sarà una diffusa crescita culturale ed una consapevolezza tecnica interna alle amministrazioni quali componenti necessarie per il successo di qualunque politica di sicurezza si voglia realizzare.
Questo percorso di medio-lungo periodo è però già in parte realizzato e monitorato attraverso il ruolo attribuito all'Agenzia per l'Italia Digitale, deputata ad emettere pareri sugli studi di fattibilità tecnica per il piano di CO (di cui il Piano di DR costituisce parte integrante) e tenuta a riferire sullo stato di attuazione del dettato normativo dell'art. 50bis del CAD.
Nella prospettiva di realizzare una resilienza della pubblica amministrazione nella sua globalità, l'adempimento degli obblighi previsti dal citato art. 50-bis significherà, allora, il raggiungimento di una capacità complessiva dell'intero sistema PA di adottare quelle misure di reazione e risposta ad eventi imprevisti che possono compromettere, anche parzialmente, il normale svolgimento delle funzioni istituzionali. La pubblica amministrazione, infatti, rappresenta un esempio di "sistema macro" all'interno del sistema paese, fortemente condizionato dall'esistenza di dipendenze dirette ed indirette tra tutte le sue componenti, a fronte delle quali solo un coordinamento unitario e l'adozione di soluzioni omogenee possono rappresentare di per sé un elemento concreto di resilienza.
All'Agenzia spetterà inoltre il compito di definire le Regole Tecniche e di Sicurezza per la realizzazione della cooperazione applicativa tra le PA, ovvero la modalità d'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi tra enti diversi; i requisiti di sicurezza ed i livelli di servizio previsti, che consentono di governare in modo uniforme, anche a livello applicativo, le interdipendenze di tipo cyber che vincolano tra loro le amministrazioni che adottano soluzioni tecniche per la l'erogazione al cittadino di servizi integrati.

Pertanto anche il tema, qui appena accennato per dovere di completezza verso quelle Amministrazioni che oltre che all'attuazione dell'art. 50 bis possono essere comunque interessate o investite da aspetti riguardanti le IC, sarà ripreso dall'Agenzia come argomento specifico da approfondire.

8 CONCLUSIONI

Come detto più diffusamente nella presente versione delle Linee Guida, l'art. 97 della Costituzione e il Codice dell'Amministrazione Digitale sanciscono che gli uffici pubblici devono essere organizzati in modo che siano garantiti la digitalizzazione dei servizi ICT, il buon funzionamento, l'efficienza e l'imparzialità.
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 a fronte 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, la disponibilità, la continuità nella fruibilità 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 dei dati uno dei cardini della sicurezza, unitamente a confidenzialità ed integrità, la disciplina della continuità operativa rappresenta parte integrante dei processi e delle politiche di sicurezza di un'organizzazione (politiche che, come si è avuto modo di evidenziare nel presente documento sono più diffusamente oggetto delle Regole tecniche previste dall'art. 51 del C.A.D., per la "Sicurezza dei dati, dei sistemi e delle infrastrutture").

In questa direzione è anche 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.
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.

L'art. 50-bis attiene alla "Continuità Operativa" e attribuisce all'Agenzia per l'Italia Digitale, anche il compito di definire linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni; con il presente documento si è inteso:

- fornire alle Amministrazioni uno strumento semplificato nello svolgimento del percorso di autovalutazione e di individuazione della soluzione di CO/DR più confacente alle caratteristiche delle Amministrazioni, destinatarie della norma;
- dare indicazioni e schemi di massima dello studio di fattibilità tecnica e dei Piani di Continuità Operativa e di Disaster Recovery, utili ai fini dell'attuazione del citato art. 50-bis.;
- completare il quadro operativo di riferimento, alla luce delle novità in materia di infrastrutture critiche;
- avviare il processo virtuoso previsto dalla norma, al fine di garantire la salvaguardia degli archivi, dei dati e delle applicazioni e l'omogeneità delle soluzioni.

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 indicate dallo strumento stesso;
- 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.

Come si è già avuto modo di evidenziare, in forza di detto articolo, attraverso la verifica annuale del costante aggiornamento dei piani di DR, ai fini dell'informativa al Ministro competente sarà possibile perseguire l'obiettivo di assicurare l'omogeneità delle soluzioni di continuità operativa.
E' affidato poi al Ministro competente il compito di informare al riguardo, con cadenza annuale, il Parlamento.

Compito dell'Agenzia sarà anche quello di aggiornare le presenti Linee Guida alla luce del procedimento di verifica richiamato e tenuto conto anche delle 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.

APPENDICE A: LE POLITICHE DI BACK UP

Indicazioni per l'attuazione di una corretta politica di backup

Predisporre le misure idonee ad impedire la distruzione e/o danneggiamento dei dati di un'Amministrazione e, comunque, rendere possibile il loro ripristino in tempi brevi senza che questo comporti delle conseguenze negative sotto il profilo economico, legale, o puramente di immagine, è compito obbligatorio per l'Amministrazione stessa.
L'Amministrazione dovrà tener conto, nell'esecuzione delle politiche di backup nonché nell'attuazione della continuità operativa, delle regole del rispettivo comparto di appartenenza per definire le modalità e i tempi di permanenza dei dati.
A tal fine, sia per una corretta gestione del sistema informativo di un Amministrazione, sia anche per l'effettiva attuazione di politiche di continuità operativa, è fondamentale eseguire procedure di backup secondo processi predefiniti per far fronte agevolmente a tutte quelle situazioni in cui sussiste un'esigenza di immediato recupero dei dati a prescindere dalla causa della loro alterazione e/o perdita (virus, guasti hardware, attacchi informatici, ecc...).

Tali processi devono rispondere ai seguenti standard:

- i dati da salvaguardare vanno raggruppati e classificati in base al periodo di conservazione (*retemption)* e alla frequenza di salvataggio;
- quando necessario, una copia del più recente backup deve essere mantenuta e prontamente disponibile per il ripristino;
- occorre predisporre opportune copie di backup che devono essere conservate in un sito protetto diverso da quello in cui risiede l'originale;
- se durante il processo di backup un file non viene salvato con successo, deve poter essere registrata tale anomalia;
- deve essere possibile verificare l'integrità dei dati salvaguardati;
- deve essere possibile salvare i dati secondo un algoritmo di cifratura;
- durante il processo di backup, se un file è in uso al momento del backup deve essere possibile eseguire successivi tentativi;
- il processo di backup deve prevedere la possibilità di eseguire backup automatici non custoditi.

Al fine di ottemperare a tali regole e a semplificare i processi di gestione, è possibile ricorrere a specifici prodotti disponibili sul mercato che automatizzano le operazioni di backup e di ripristino; le specifiche scelte organizzative e di processo devono essere rappresentate all'interno del Piano di CO (e, per la parte di propria competenza, nel Piano di Disaster Recovery), oltre che all'interno dei documenti adottati dalle Amministrazioni per l'adozione di misure di sicurezza, avendo cura di rendere allineati i dati nei sopra citati documenti. Le politiche di backup normalmente contemplano, in relazione al dato da salvaguardare, vari tipi di salvataggio dei dati, ognuno dei quali trova specifici campi di applicazione:

- full backup: backup completo dei dati indicati;
- backup incrementale: backup che salva solo le modifiche apportate ai dati rispetto all'ultimo salvataggio incrementale compiuto;
- backup differenziale: backup cumulativo di tutti i cambiamenti apportati rispetto all'ultimo full backup;
- disk image: metodo di backup di un intero disco o di un file system;
- hot backup: salvataggio di un database effettuato mentre il database e/o il file è aperto ed in fase di aggiornamento;
- cold backup: salvataggio di un database effettuato mentre il database e/o il file è chiuso e non sottoposto ad aggiornamento.

I sistemi sono tipicamente i server e i sottosistemi dischi ma potrebbero riguardare anche altri componenti che contengono dati.
I server dei sistemi oggetto di backup devono, oltre ai dati utente, includere: le configurazioni, i sistemi operativi, i prodotti, i file server, i server di posta e i web server.
Ciascun backup deve essere raggruppato in un set autoconsistente (ad esempio un full backup settimanale + 7 backup incrementali giornalieri = un set di backup) e rappresenta l'unità da utilizzare in caso di ripristino dei dati.
Una politica di backup deve essere composta almeno dalle sezioni descrittive di seguito illustrate.

Scopo

Definire il perimetro dei sistemi a cui la politica si riferisce, l'ufficio o l'organizzazione a cui i sistemi sono associati.

Tempistica

La tempistica è la periodicità con cui vanno eseguiti i salvataggi dei dati. Si possono avere due tipologie di backup: di tipo totale (*full backup*) o di tipo incrementale (*incremental backup*).
Per esempio:

Periodicità	Tipo backup
Settimanale	Totale
Giornaliero	Incrementale
Mensile	Totale

Periodo di ritenzione

I salvataggi devono avere un periodo di ritenzione passato il quale vengono eliminati, periodo commisurato alle finalità della conservazione dell'informazione (dei dati, delle applicazioni e dei processi). Tale periodo deve essere precisamente indicato in tutti i documenti interessati (in particolare nel Piano di Continuità Operativa (PCO) e nel Piano di Disaster Recovery (PDR)). A titolo di esempio si riportano alcune periodicità:

Periodicità	Tipo	Ritenzione
Settimanale	Totale	2 settimane
Giornaliero	Incrementale	7 giorni
Mensile	Totale	6 mesi

Il periodo di ritenzione consente il recupero periodico degli spazi o dei supporti usati per il salvataggio dei dati.

Responsabilità

Deve essere identificata la funzione o la divisione responsabile per l'esecuzione delle procedure relative alla politica di backup.

Verifica salvataggi

Periodicamente la politica deve prevedere di effettuare un ripristino dei dati salvati per verificare la bontà dei backup effettuati.

Lista dei dati salvati

Devono essere elencati tutti i dati, gli archivi e i log, oggetto del salvataggio a cui la politica fa riferimento.

Archiviazioni

La politica deve prevedere che periodicamente tutti o parte dei dati salvati siano oggetto di archiviazione su dispositivi che ne preservano l'integrità per periodi commisurati alle finalità di conservazione delle informazioni precisamente indicati nei documenti interessati (PCO, PDR), prevedendo le misure di conservazione relative al mantenimento dell'efficiente funzionalità del sistema informativo. Ai fini delle politiche di archiviazione storico documentale, le Amministrazioni si dovranno attenere a quanto definito nell'ambito del "Manuale di Conservazione" che ne contiene le regole e i tempi.

Ripristino (Restore)

La politica di backup deve contenere l'insieme delle procedure da eseguire in caso di ripristino dei dati, in termini di modalità, sequenza e controllo dei dati ripristinati

Ubicazione

In caso di uso di supporti removibili di salvataggio, la politica deve prevedere il tipo di conservazione e l'ubicazione dei supporti (armadi ignifughi, caveau ecc…).
Inoltre il sistema di backup deve rispondere alle seguenti caratteristiche:

- il sistema deve gestire ed interfacciarsi con sistemi complessi come ad esempio Database, con soluzioni di messaging ed ERP per effettuare backup e restore coerenti dei sistemi gestiti;
- il sistema di Backup/Restore deve effettuare il cloning di sistemi permettendo di pianificare soluzioni di Disaster Recovery;
- il sistema di backup centralizzato deve permettere la gestione automatica dei media, il "cartridge cleaning", il labeling elettronico, la gestione dei bar code e la verifica dei media;
- il sistema di Backup e restore di dati deve avvenire attraverso una rete separata creando opportune segregazioni con sottoreti virtuali o con rete e relativi apparati dedicati. Le porte di comunicazione dei sistemi di backup devono essere protetti da reti considerate non sicure attraverso adeguati filtri di comunicazione IP;
- le informazioni memorizzate su supporti utilizzati per il backup devono essere cifrati (esempio: AES).

Si sottolinea che, in relazione all'impiego di tecniche di cifratura, è necessario che queste non pregiudichino la disponibilità dei dati in caso di necessità, e che, pertanto, sia assicurata a tale scopo la compatibilità tecnologica dei supporti, dei formati di registrazione, degli strumenti crittografici e degli apparati di lettura dei dati per tutta la durata della conservazione del dato.

APPENDICE B: GLI 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.
In questa appendice si prendono a riferimento solo gli standard ISO (nelle due accezioni di seguito rappresentate), che in modo diretto o indiretto rappresentino riferimenti per la continuità operativa. Fa eccezione il quadro di riferimento costituito dall'ITIL, che serve a introdurre brevi note sullo standard ISO 20000.

Tipologie di "standard"

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. Nello specifico della continuità operativa (in senso generale e nel senso di continuità operativa ICT) gli "standard" 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.

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.
Per comodità di lettura possiamo distinguere le seguenti tipologie di standard ISO su questo tema:

- Standard ISO relativi alla continuità operativa generale dell'organizzazione
    - ISO 22313 e ISO 22301 – sistema di gestione della CO generale
- Standard ISO/IEC relativi alla CO e al DR ICT
    - ISO/IEC 27031 relativo alla CO ICT
    - ISO/IEC 24762 relativo ai servizi di DR ICT
- Standard ISO/IEC relativi a tematiche ICT correlate alla CO e al DR
    - ISO/IEC 27001 e 27002 relative alla sicurezza ICT che prevedono tra gli oggetti di controllo la gestione della continuità operativa
    - ISO/IEC 20000-1 e 20000-2 relative al sistema di gestione dei servizi ICT che include tra i servizi la gestione della continuità dei servizi

Lo standard più importante, ufficializzato nel maggio 2012, è la norma ISO 22301.

Gli standard ISO 22301 e ISO 22313

L'ISO adotta le due versioni di uno standard, una per le "buone pratiche" e la seconda per i processi di verifica e, quindi, di certificazione.
Tale atteggiamento vale anche per gli standard relativi alla CO e, infatti, ha predisposto uno schema a due standard:

- lo standard **ISO 22301** ("Societal security -- Buisiness continuity management systems – Requirements"), emesso nel maggio 2012 tratta del sistema di gestione della CO e delle verifiche, che implica un percorso di certificazione
- lo standard **ISO 22313** ("Societal security. Business continuity management systems. Guidance"), emesso nel dicembre 2012, descrive le buone pratiche in materia di CO. Costituisce una guida per la ISO 22301, aiutando le organizzazioni che intendono realizzare efficaci sistemi di gestione della CO.

Questi standard sono di competenza del Technical Committee 223 dell'ISO ("Societal Security"), che ha per finalità proprio la produzione di standard per la gestione delle crisi.
Va sottolineato che, benché siano la base più importante, i contenuti dello standard del BSI[6] BS 25999, questi non sono gli unici che hanno contribuito al lavoro dell'ISO. Vi sono infatti contributi provenienti da Australia, Giappone, Israele, dalla Svezia e dagli Stati Uniti.
Inoltre, mentre il BS 25999 pone l'accento sulla pura continuità delle attività specifiche di un'organizzazione (nell'espressione "business continuity" il termine "business" ha un'accezione che va oltre il significato della parola "affari"), l'ISO preferisce parlare di "preparedness and continuity", volendo così fornire una visione più generale della continuità, non limitata alla sola protezione delle attività dell'organizzazione. Infatti si utilizza l'espressione di "sicurezza sociale" e ci si riferisce ad altri aspetti della sicurezza civile. Va anche detto che la presenza in vari altri contesti di standard del tema della continuità operativa non semplifica il prospetto della visione dell'ISO. Si possono infatti citare dai trenta ai quaranta standard presenti o in progetto che, in un modo o nell'altro comprendono anche questo tema. In definitiva, la visione complessiva dell'ISO sulla continuità operativa è un processo ancora in corso e, per ora, non eccessivamente influente sulle imprese.
Volendo istituire un raffronto fra le indicazioni riportate nelle Linee Guida e lo standard ISO 22301, si evidenzia schematicamente quanto segue:

LG DigitPA	**ISO 22301**
Coinvolgimento dei vertici dell'amministrazione e ruolo della struttura di gestione	5.1 - Leadership and commitment
Criteri e Indicazioni Organizzative	5.4 - Organizational roles, responsibilities and authorities
Strumenti per l'autovalutazione	8.2.2 – BIA
Il Comitato di crisi	8.4.2 - Incident response structure
Indicazioni per il collaudo e per i test	8.5 – exercising and testing
Indicazioni per Il Piano di Continuità Operativa Il Piano di Continuità Operativa	8.4.4 Business continuity plans
Indicazioni per la gestione e la manutenzione della soluzione di CO/DR e del Piano di CO/DR	10.1 Nonconformity and corrective action

[6] British Standard Institute, l'organizzazione che rappresenta il riferimento per gli standard nel Regno Unito

Lo standard ISO/IEC 24762

Nel 2008 l'ISO ha pubblicato un nuovo standard (del tipo "buone pratiche") che fornisce le indicazioni per i servizi di Disaster Recovery dell'ICT: lo standard **ISO/IEC 24762** ("Information technology — Security techniques — Guidelines for information and communications technology Disaster Recovery services").
Questo standard copre i seguenti aspetti:

- messa in opera, gestione, supervisione e manutenzione delle infrastrutture e dei servizi per il Disaster Recovery;
- le esigenze per la fornitura dei servizi e delle infrastrutture del Disaster Recovery;
- i criteri di selezione dei siti alternativi;
- le attività per il miglioramento continuo dei servizi e delle prestazioni del Disaster Recovery.

Sulla base di questo standard è possibile definire i requisiti per un servizio di Disaster Recovery, erogati internamente o da fornitori esterni, e, pertanto, lo standard costituisce un ottimo punto di riferimento per la costruzione di gare destinate alla ricerca di un servizio di Disaster Recovery.

Lo standard ISO/IEC 27031

Nel marzo 2011 è stato pubblicato lo standard **ISO/IEC 27031** ("Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity").
Il campo di applicazione dello standard norma ISO / IEC 27031:2011 comprende tutti gli eventi (tra cui quelli correlati alla sicurezza), che potrebbero avere un impatto sulle infrastrutture e sistemi ICT e include ed estende la pratica della gestione dei problemi della sicurezza delle informazioni e la gestione e la disponibilità dei servizi ICT.
Lo standard fornisce un collegamento tra gestione generale della continuità operativa e delle tecnologie dell'informazione, fornendo una visione che mette insieme BS 25999, ISO/IEC 24762 e ISO 27001. Lo standard dà quindi un quadro di riferimento e dei metodi di processo di identificazione e di specificazione di tutti gli aspetti per migliorare la preparazione dell'ICT dell'organizzazione alle emergenze, garantendo quindi la continuità dell'organizzazione stessa.

Lo standard della sicurezza ISO/IEC 27002

Questo standard ("Information technology -- Security techniques -- Code of practice for information security management"), piuttosto noto, rappresenta, con lo standard ISO/IEC 27001 ("Information technology -- Security techniques -- Information security management systems – Requirements", che è utilizzato per un percorso di certificazione), uno dei primi standard dedicati alla sicurezza informatica sotto il profilo dei processi. Lo standard contiene raccomandazioni concrete per garantire la sicurezza delle informazioni, più precisamente il processo di messa in sicurezza. Comprende nove capitoli che trattano i differenti aspetti riguardanti la sicurezza.

Il capitolo 14 dello standard 27002 tratta della "gestione del piano di continuità dell'attività" per circa due pagine, affrontando, quindi, l'argomento a un livello piuttosto alto.

Le pratiche correlate alla continuità operativa

Oltre all'insieme degli specifici standard dedicati al tema della continuità operativa e al Disaster Recovery esistono quadri di riferimento e standard che hanno al loro interno qualche riferimento alla CO. E' il caso dell'ITIL ("Information Technology Infrastructure Library"), che è un insieme di pratiche e raccomandazioni per la gestione dei servizi informatici sotto forma di pubblicazioni (a oggi oltre 30). I nomi "ITIL" e "IT Infrastructure Library" sono marchi registrati dell'United Kingdom's Office of Government Commerce (OGC).

L'ITIL, giunto alla versione 3, prevede 5 processi base per la gestione di un'infrastruttura informatica:

- Service Strategy;
- Service Design;
- Service Transition;
- Service Operation;
- Continual Service Improvement.

Nell'ambito dei "Service Design" è dedicato al tema della CO un capitolo specifico, "IT Service Continuity Management", nel quale sono indicati appositi KPI (key performance indicator), utili per la valutazione dello stato della CO e del Disaster Recovery di un'organizzazione, di seguito riportati:

Key Performance Indicator (KPI)	**Definition**
Business Processes with Continuity Agreements	Percentage of business processes which are covered by explicit service continuity targets
Gaps in Disaster Preparation	Number of identified gaps in the preparation for disaster events (major threats without any defined counter measures)
Implementation Duration	Duration from the identification of a disaster-related risk to the implementation of a suitable continuity mechanism
Number of Disaster Practices	Number of disaster practices actually carried out
Number of Identified Shortcomings during Disaster Practices	Number of identified shortcomings in the preparation for disaster events which are identified during practices

Lo standard ISO/IEC 20000:2011

Nel 2005 è stata emanata la norma ISO/IEC 20000, che traspone nell'ambito delle norme internazionali riferite a processi di certificazione i concetti relativi alla realizzazione e gestione di servizi IT di qualità che soddisfino i requisiti e le esigenze del committente. Nel 2011 la norma è stata aggiornata e già nell'uso nel titolo ("Service management system requirements") dell'espressione "service management" al posto di "IT service management" (titolo della norma nella versione 2005), l'attenzione alla filosofia del servizio in generale piuttosto che limitata al solo IT.

Riguardo ai temi tipici della continuità operativa, la norma contiene specifici riferimenti alla continuità dei servizi contenuti nel capitolo 6.3 "Service Continuity and Availability Management" e nei paragrafi 6.3.1 "Service Continuity and Availability requirements", 6.3.2 "Service Continuity and Availability plans" e 6.3.3 "Service Continuity and Availability monitoring and testing".

APPENDICE C: MODELLO DI PIANO DI CONTINUITA' ICT

NOTA INTRODUTTIVA AL MODELLO

Il Piano di Continuita' Operativa ICT (nel seguito, semplicemente PCO) è un documento complesso, articolato in più sezioni, che può contenere al suo interno documentazione di natura diversa come procedure operative, organizzative, schede, elenchi di persone e di materiale, istruzioni operative, eccetera.

L'eventuale documentazione a completamento del presente documento deve essere predisposta secondo un criterio di facile reperibilità.

Una tabella riassuntiva di tutta la documentazione può aiutare al reperimento facile ed immediato della documentazione da includere o allegare al PCO.

E' di fondamentale importanza che tutta la documentazione relativa al PCO sia stata gia' approvata dalla dirigenza dell'Amministrazione, soprattutto la documentazione che conferisce gli opportuni poteri e responsabilita' alle varie figure (Comitato di crisi ICT e Responsabile della Continuita' Operativa ICT) durante la fase di emergenza.

Il PCO si compone di attività e fasi che devono essere dettagliatamente specificate e descritte. É utile in ogni caso avere una visione complessiva dell'intero flusso di attività in modo che ciascun soggetto coinvolto abbia immediatamente evidenza delle interazioni tra le singole fasi.

Il PCO rappresenta pertanto una guida generale che indica come reagire ad eventi "negativi" di significativa rilevanza, che determinano l'indisponibilità di quei processi/servizi critici di cui si garantisce il ripristino entro determinati limiti di tempo.

Il PCO prevede l'esecuzione di chiare ed efficaci azioni (formalizzate in procedure, istruzioni operative, atti e documenti), da parte dei soggetti coinvolti nel piano, come completa risposta alla situazione d'emergenza, all'eventuale stato di emergenza, e sono finalizzate al ripristino dei servizi sino al rientro alla situazione di normalità.

Tali azioni dovranno essere eseguite da ciascun soggetto con immediatezza, in considerazione degli obiettivi da perseguire. Inoltre, nell'ambito della struttura organizzativa per il PCO predisposta da codesta Amministrazione il Responsabile della Continuita' Operativa ICT assume un ruolo strategico, sia in condizioni ordinarie sia in eventuali condizioni di emergenza, per assicurare il coordinamento delle operazioni e il mantenimento, aggiornamento e sviluppo futuro del PCO.

Obiettivo del Piano di Continuità Operativa ICT

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

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

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

- Piano di Protezione Civile, secondo Ordinanza del Presidente del Consiglio dei Ministri del 28 agosto 2007, n. 3606,

- Piano di Emergenza, secondo DL 81/2008.

Si precisa, però, che il Piano è stato comunque verificato come coerente con le suddette normative.
Benché il presente Piano rappresenti una specifica realizzazione nel contesto di quanto previsto dall'articolo 50-bis del CAD e non sia, quindi, direttamente riconducibile a un preciso standard, sono norme internazionali di riferimento le seguenti:

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

Definizioni e abbreviazioni

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

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

Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

- i vertici dell'Amministrazione;
- il responsabile della CO ICT, così come indicato nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011;
- il personale dell'Amministrazione di qualunque tipologia (fruitore o gestore) direttamente coinvolto nell'IT dell'Amministrazione;
- la comunità di riferimento territoriale e sociale (cittadini e imprese) dell'Amministrazione;
- le organizzazioni e/o istituzioni che interagiscono con l'Amministrazione in modalità informatiche;
- se presenti, tutti i fornitori, a qualunque titolo, di attività di supporto informatico.

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

In data ….l'Amministrazione ha presentato richiesta di parere, così come previsto dal comma 4 dell'articolo 50-bis del CAD.
In data ….AGID ha emesso parere "favorevole"/"favorevole condizionato".

I servizi in ambito nello SFT

I servizi in ambito identificati nello SFT CON I RELATIVI LIVELLI (Tier) di criticità sono stati seguenti:
Inserire tabella punto 5.2 SFT comprensiva anche di RPO e RTO e senza presenza/assenza soluzione.
L'Amministrazione ha ritenuto, invece, non in ambito, i seguenti servizi:
Inserire tabella con i servizi non ritenuti in ambito

La sintesi del parere di AGID.

PQM del parere rilasciato.

Variazioni eventuali nel numero dei servizi e relative criticità.

Inserire la tabella punto 5.2 SFT con aggiunte/modifiche o indicazione di "nessuna variazione"

Sintesi di informazioni organizzative e tecniche sull'Amministrazione

Matrice servizi/organizzazione (responsabilità)

In questo paragrafo devono essere individuati, sulla base dei servizi facenti parte del perimetro del piano della continuità operativa, l'ufficio responsabile, il nome del responsabile della erogazione del servizio stesso.

SERVIZIO	UFFICIO RESPONSABILE	RESPONSABILE
A		
B		
….		

Matrice servizi/infrastruttura tecnologica

Per ogni servizio deve essere indicato:

- *Nel campo "Sistema(i) di esercizio"*
  - *se il servizio è esternalizzato, oppure*
  - *se il servizio è interno all'amministrazione, nel qual caso vanno indicati in modo puntuali i sistemi hw e sw che rendono operativo il servizio;*
- *Nel campo "Localizzazione" il luogo fisico in cui risiedono i sistemi che concorro alla erogazione del servizio;*
- *Nel campo "LDS" le clausole contrattuali previste per la prestazione del servizio se in carico ad un fornitore, altrimenti gli obiettivi di prestazione del servizio in termini di orario durante il quale deve essere assicurata l'erogazione del servizio.*

In caso di servizio composto da più servizi devono essere chiaramente riportate le relazioni tra i servizi: ogni servizio componente dovrà rientrare nell'ambito di applicabilità del PCO.

SERVIZIO	SISTEMA(I) DI ESERCIZIO	LOCALIZZAZIONE	LDS (orario disponibilità)
A			
B			
….			

Predisposizione all'emergenza

In questo capitolo deve essere descritta la struttura organizzativa preposta per il PCO con l'attribuzione di ruoli e responsabilità alle singole risorse coinvolte nel Piano, le liste di reperibilità e contatti.

La struttura organizzativa

Comitato di crisi ICT

Responsabile della Continuità Operativa ICT

Strutture tecniche

Se esistenti

Composizione, ruoli, procedure operative

Gestione delle reperibilità

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

Soluzione di continuità

*I paragrafi che seguono devono essere redatti per **ogni servizio in ambito** (dopo la revisione iniziale dei servizi e le eventuali variazioni). Se le caratteristiche organizzative, procedurali e tecniche sono comuni a più servizi, i contenuti che seguono andranno riferiti a tutti questi servizi, indicandoli nell'intestazione.*

Interrelazioni del servizio/i con entità esterne all'Amministrazione

Per ogni entità coinvolta devono essere descritte le interrelazioni col servizio A e come queste entità possono condizionare e/o essere coinvolte in caso di disastro (altre PA, fornitori, compagnie di assicurazioni, ecc.).

ENTITA'	DIREZIONE FLUSSI

Dati logistici generali

Contiene dati quali:

- *dove andare (ubicazione del sito alternativo);*
- *come si accede al sito (percorsi stradali, ferroviari,; parcheggi; ecc.);*
- *autorizzazioni necessarie per accedervi;*
- *….*

Nel caso di servizio esternalizzato dei paragrafi che seguono vanno redatti solo i paragrafi "Posti di lavoro" e "SLA o accordi di servizio specifici"

Dati infrastrutturali

Contiene dati relativi alla esatta localizzazione fisica e impiantistica nella quale è esercita la soluzione per il/i servizio/i in questione.

Dati logistici specifici

Contiene dati relativi alla precisa localizzazione, all'interno del sito alternativo, dell'ambiente nel quale è esercita la soluzione di continuità.

Infrastrutture di continuità e protezione fisica

Contiene dati relativi alla localizzazione del punto precedente o all'intera infrastruttura del sito alternativo, punto quali:

- *caratteristiche sistemi di alimentazione e di continuità elettrica;*
- *caratteristiche sistemi di raffreddamento;*
- *caratteristiche sistemi antincendio e antifumo;*
- *caratteristiche sistemi anti allagamento;*
- *.....*

Controllo fisico degli accessi (impianti e procedure)

Contiene dati relativi alle modalità di accesso fisico (tornelli, porte ad accesso controllato, ecc.) e relative procedure di gestione e ai sistemi di videosorveglianza e relative procedure all'area del sito alternativo (o all'intero sito alternativo) dedicata alla soluzione di continuità.

Ambiente logistico (interno) per la continuità

Contiene dati sugli asset disponibili presso il sito alternativo (uffici, sale riunioni, impianti di fonia, aree per le postazioni di lavoro, ecc.).

Apparati hw e postazioni di lavoro

Descrizione delle risorse elaborative e di storage dedicate alla soluzione. Contiene anche le caratteristiche delle postazioni di lavoro (numero, tipologia, procedure per la gestione in caso di normalità e in caso di emergenza, ecc.) Nominativo del fornitore/i dell'assistenza e relativi SLA.
Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

Sw ambiente

Descrizione del sw di ambiente (sistema operativo, ambiente DB, ecc.). Nominativo del fornitore/i dell'assistenza e relativi SLA.
Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

Sw applicativo

Descrizione delle applicazioni che supportano la soluzione di continuità. Nominativo del fornitore/i dell'assistenza e relativi SLA.

Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

Rete interna

Descrizione della rete interna (cablaggio, router, switch, firewall, ecc.). Nominativo del fornitore/i dell'assistenza e relativi SLA.

Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

Rete esterna

Descrizione dei collegamenti geografici (caratteristiche, fornitore,SLA, ecc.).
Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

Istruzioni operative di start up dei servizi

Contiene le indicazioni per:

- *l'attivazione dei sistemi hw e sw dedicati alla continuità;*
- *l'attivazione operativa del servizio/i.*

Gestione dei sistemi hw, sw, di rete in situazione di normalità

Contiene la descrizione dell'impiego e della gestione dei sistemi dedicati alla soluzione in caso di normalità, con particolare attenzione alla verifica del corretto allineamento dei dati e delle configurazioni tra sito primario e sito secondario di DR.

Dati procedurali

Contiene dati relativi alle fasi e alle procedure impiegate per la soluzione di continuità del servizio/i in caso di emergenza.

Scenari di emergenza applicabili

In questo capitolo verranno riportati un riassunto degli scenari individuati durante lo studio di fattibilita' con i relativi RTO e RPO.

Fase di reazione all'emergenza

Le attività previste dal PCO in caso di "reazione" ad un evento negativo di portata "disastrosa" rientrano in quello che si definisce "Processo di reazione all'emergenza".
La descrizione dettagliata delle attivita' che compongono tale Processo sono parte preponderante del PCO poiché descrivono "chi fa cosa" dal momento della Reazione all'emergenza fino al Ritorno allo Stato di Normalità.
In questa fase si raccolgono le segnalazioni di incidente. Ciascun evento deve essere analizzato e in caso di gravita' deve essere informato il Responsabile della Continuita' Operativa che ne esamina la criticità e ne stima la gravità. Sarà suo compito valutare se l'evento è tale da generare una possibile situazione di emergenza e, quindi coinvolgere il Comitato di crisi ICT, oppure se l'evento va gestito con le "normali" procedure di gestione degli incidenti.
In questa fase il Comitato di crisi ICT sancisce ufficialmente l'entrata nello Stato di Emergenza e deve essere previsto l'invio delle diverse notifiche ai vertici dell'Amministrazione, al personale dell'Amministrazione, ai fornitori e agli altri soggetti che si ritiene opportuno coinvolgere. Le notifiche inviate ai Team di ICT costituiranno l'avvio ufficiale delle operazioni di riattivazione e rientro. Devono essere inoltre descritte in questo capitolo le modalità alternative di comunicazione da adottare nel caso in cui la modalità primaria non sia disponibile. Nel corso di questa fase è inoltre necessario provvedere tempestivamente alla reazione all'emergenza stessa e per questo motivo è necessario definire le diverse modalità di escalation da seguire a fronte di specifici eventi negativi.
I passi da seguire sono:

- *Segnalazione dell'emergenza*

- *Valutazione della criticità*
- *Attivazione del comitato gestione della crisi ICT*
- *Modalità di gestione dell'emergenza, che contiene dati quali:*
    - *trasferimento del personale;*
    - *occupazione del sito alternativo;*
    - *innesco del piano di DR;*
    - *chi deve andare a casa e chi deve trasferirsi nel sito alternativo,*
    - *cosa deve fare il personale presso il sito alternativo,*
    - *cosa non deve fare il personale presso il sito alternativo,*
    - *.....*

Fase di gestione dell'emergenza e riattivazione dei servizi

Le attività prioritarie, successivamente alla notifica dello stato di emergenza, sono comunque quelle di ripristino dei servizi sul sito secondario di Disaster Recovery. Devono quindi essere descritte le procedure che il Team di ICT dovrà eseguire per lo start-up dei sistemi e verifica degli allineamenti (dichiarando così il momento a partire dal quale si sono persi i dati) e di attivazione e test di tutti i servizi in DR. Infine, successivamente alla dichiarazione di "sistemi up & running", deve essere definito come notificare il passaggio sul sito secondario (tale notifica è necessaria per la verifica del rispetto del parametro di RTO).

Durante lo Stato di emergenza è probabile che sia necessario operare utilizzando modalità alternative anche per le attività di acquisto di materiale/strumenti e/o di gestione delle trasferte dei dipendenti. Per queste finalità è necessario quindi redigere delle procedure specifiche. Dovranno infine essere previste procedure per la comunicazione verso il personale, i soggetti terzi coinvolti ed eventualmente i media.

I passi da seguire sono:

- *Modalità di dichiarazione dello stato di emergenza*
- *Comunicazione al personale (reperibile, altro personale)*
- *Comunicazione ai mezzi di comunicazione e ai soggetti terzi sullo stato di emergenza*
- *Modalità di notifica all'azienda (fornitore) che ha stipulato il contratto di fornitura di servizi per il DR*
- *Dichiarazione servizi attivi su sito di DR*

Fase di ritorno alla normalità

In questa fase è necessario valutare le possibili strategie di rientro e scegliere se rientrare sul sistema primario oppure promuovere il sito secondario a primario. Vista la natura strategica della scelta è necessario il coinvolgimento del Comitato di crisi ICT. In funzione della strategia individuata il personale ICT si adopererà per garantire il rientro sul primario o sul secondario (che diventa primario) con livelli di performance normali. Al termine una fase di test verificherà che il rientro sia avvenuto in maniera efficace. Una notifica formale decreterà il rientro alle condizioni di normale operatività. Dovrà poi essere prevista una attività di reportistica per registrare quanto accaduto ed analizzarlo successivamente per valutare l'efficacia del PCO ed eventualmente provvedere al suo aggiornamento.

I passi da seguire sono:

- *Analisi dei danni*
- *Organizzazione e pianificazione delle attività di rientro*
- *Reportistica (descrizione emergenza, descrizione test di verifica rientro)*

Formazione

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

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

Gestione e aggiornamento del piano di continuita' operativa

Il PCO non è un documento statico e, pertanto, è necessario pianificare, all'interno del PCO stesso, sia le modalità di verifica dei contenuti (test), sia le modalità di revisione e aggiornamento.
Per quanto attiene ai test, sono possibili varie modalità di test:

- *una semplice verifica dell'effettiva disponibilità di tutto quanto si renderebbe necessario in caso di emergenza (nomina responsabile CO, nomina Comitato di crisi ICT, gestione delle reperibilità, disponibilit e funzionamento degli impianti del sito secondario, disponibilità delle risorse elaborative e di rete, ecc.). In questo caso va preventivamente predisposta una cheklist che permetta di verificare quanto sopra. Questo tipo di test non garantisce che in caso di emergenza non ci siano funzionalità non in linea con quanto previsto, ma è facilmente eseguibile;*
- *un test cosiddetto "walkthrough": questo tipo di test si svolge con una simulazione (cioè, senza attivazione fisica dei sistemi) fatta da tutto il personale da coinvolgere previsto dal PCO. Deve essere preparato con cura, soprattutto per descrivere lo scenario di crisi ipotetico verso il quale ciascun partecipante, secondo il ruolo che ha nel PCO, esegue le procedure previste per ognuna delle fasi indicate. Anche se più complesso da organizzare rispetto alla semplice verifica della disponibilità di risorse e impianti, questo test non implica l'attivazione dei sistemi alternativi e può essere un modo utile anche per la formazione e la verifica della preparazione del personale;*
- *test degli impianti e delle risorse: in questo caso non solo le procedure, ma anche l'effettiva attivazione delle risorse fisiche e IT viene verificata, sempre a fronte della simulazione di un'emergenza. Un test di questo tipo richiede una attenta predisposizione e un sensibile impegno per il personale, ma garantisce la reale verifica della soluzione di continuità del PCO. Per ognuna delle fasi dell'emergenza vanno programmate ed eseguite le attività previste.*

Collegato al tipo di test degli impianti, è il test effettuato senza preavviso delle risorse interessate. Si tratta di una possibilità realmente fattibile solo in presenza di una alto livello di professionalità delle figure coinvolte. Naturalmente, un simile test si avvicina a quanto effettivamente potrebbe prodursi in caso di emergenza e permette un livello di garanzia della funzionalità della soluzione di continuità estremamente alto.
E' necessario, al minimo, eseguire almeno un test all'anno.

Quanto all'aggiornamento e alle revisioni da fare per il PCO, vanno segnalate nello stesso le condizioni ordinarie che si possono verificare determinando cambiamenti organizzativi, tecnici, logistici, procedurali che hanno effetti rilevanti su una o più parti del Piano.

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

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

Il verificarsi di uno di questi eventi, o comunque di un qualsiasi evento che può incidere sull'efficacia del PCO, richiede quindi un'attenta analisi per valutare la necessità di attuare delle modifiche al Piano, cioè di un suo adeguamento.

E' comunque necessario che almeno una volta all'anno, in concomitanza o meno con il test, il Comitato di crisi si riunisca per analizzare la completezza e attualità del PCO.
I settori nel PCO che danno evidenza di queste attività sono i seguenti:

Modalità di esecuzione dei test periodici
Modalità di revisione e adeguamento del piano

APPENDICE D: SPECIFICAZIONI SUGLI STRUMENTI GIURIDICI ED OPERATIVI PER L'ACQUISIZIONE DEI SERVIZI DI CO/DR

D.1 INDICAZIONI DI DETTAGLIO SULLE NORME PER L'ACQUISIZIONE DEI SERVIZI

Le modalità di aggregazione della domanda e dell'offerta

Si coglie l'occasione per ricordare che nell'ambito del citato "Codice dei contratti" l'articolo 33, così come innovato dalla già citata L. n. 135/2012, e che attiene a "Appalti pubblici e accordi quadro stipulati da centrali di committenza", prevede:

1. *Le stazioni appaltanti e gli enti aggiudicatori possono acquisire lavori, servizi e forniture facendo ricorso a centrali di committenza, anche associandosi o consorziandosi.*

2. *Le centrali di committenza sono tenute all'osservanza del presente codice.*

3. *Le Amministrazioni aggiudicatrici e i soggetti di cui all'articolo 32, c. 1, lettere b), c), f),*[7] *non possono affidare a soggetti pubblici o privati l'espletamento delle funzioni e delle attività di stazione appaltante di lavori pubblici. Tuttavia le Amministrazioni aggiudicatrici possono affidare le funzioni di stazione appaltante di lavori pubblici ai servizi integrati infrastrutture e trasporti (SIIT) o alle Amministrazioni provinciali, sulla base di apposito disciplinare che prevede altresì il rimborso dei costi sostenuti dagli stessi per le attività espletate, nonché a centrali di committenza.*

---

[7] ***Art. 32. Amministrazioni aggiudicatrici e altri soggetti aggiudicatori***

(artt. 1 e 8, dir. 2004/18; art. 2, legge n. 109/1994; art. 1, d.lgs. n. 358/1992; artt. 2 e 3, co. 5, d.lgs. n. 157/1995)

1. Salvo quanto dispongono il comma 2 e il comma 3, le norme del presente titolo, nonché quelle della parte I, IV e V, si applicano in relazione ai seguenti contratti, di importo pari o superiore alle soglie di cui all'articolo 28:

a) lavori, servizi, forniture, affidati dalle amministrazioni aggiudicatrici;

b) appalti di lavori pubblici affidati dai concessionari di lavori pubblici che non sono amministrazioni aggiudicatrici, nei limiti stabiliti dall'articolo 142;

c) lavori, servizi, forniture affidati dalle società con capitale pubblico, anche non maggioritario, che non sono organismi di diritto pubblico, che hanno ad oggetto della loro attività la realizzazione di lavori o opere, ovvero la produzione di beni o servizi, non destinati ad essere collocati sul mercato in regime di libera concorrenza, ivi comprese le società di cui agli articoli 113, 113-bis, 115 e 116 del decreto legislativo 18 agosto 2000, n. 267, testo unico delle leggi sull'ordinamento degli enti locali;

(lettera da coordinare con l'art. 13 della legge n. 248 del 2006 - n.d.r.)

d) lavori, affidati da soggetti privati, di cui all'allegato I, nonché lavori di edilizia relativi ad ospedali, impianti sportivi, ricreativi e per il tempo libero, edifici scolastici e universitari, edifici destinati a funzioni pubbliche amministrative, di importo superiore a un milione di euro, per la cui realizzazione sia previsto, da parte dei soggetti di cui alla lettera a), un contributo diretto e specifico, in conto interessi o in conto capitale che, attualizzato, superi il 50 per cento dell'importo dei lavori;

e) appalti di servizi, affidati da soggetti privati, relativamente ai servizi il cui valore stimato, al netto dell'i.v.a., sia pari o superiore a 200.000 euro, allorché tali appalti sono connessi ad un appalto di lavori di cui alla lettera d) del presente comma, e per i quali sia previsto, da parte dei soggetti di cui alla lettera a), un contributo diretto e specifico, in conto interessi o in conto capitale che, attualizzato, superi il 50 per cento dell'importo dei servizi;

f) lavori pubblici affidati dai concessionari di servizi, quando essi sono strettamente strumentali alla gestione del servizio e le opere pubbliche diventano di proprietà dell'amministrazione aggiudicatrice;

g) lavori pubblici da realizzarsi da parte dei soggetti privati, titolari di permesso di costruire, che assumono in via diretta l'esecuzione delle opere di urbanizzazione a scomputo totale o parziale del contributo previsto per il rilascio del permesso, ai sensi dell'articolo 16, comma 2, del d.P.R. 6 giugno 2001, n. 380, e dell'articolo 28, comma 5 della legge 17 agosto 1942, n. 1150. L'amministrazione che rilascia il permesso di costruire può prevedere che, in relazione alla realizzazione delle opere di urbanizzazione, l'avente diritto a richiedere il permesso di costruire presenti all'amministrazione stessa, in sede di richiesta del permesso di costruire, un progetto preliminare delle opere da eseguire, con l'indicazione del tempo massimo in cui devono essere completate, allegando lo schema del relativo contratto di appalto. L'amministrazione, sulla base del progetto preliminare, indice una gara con le modalità previste dall'articolo 55. Oggetto del contratto, previa acquisizione del progetto definitivo in sede di offerta, sono la progettazione esecutiva e le esecuzioni di lavori. L'offerta relativa al prezzo indica distintamente il corrispettivo richiesto per la progettazione definitiva ed esecutiva, per l'esecuzione dei lavori e per gli oneri di sicurezza;

(lettera così modificata dall'art. 1, comma 1, lettera f), d.lgs. n. 152 del 2008)

h) lavori, servizi forniture affidati dagli enti aggiudicatori di cui all'articolo 207, qualora, ai sensi dell'articolo 214, devono trovare applicazione le disposizioni della parte II anziché quelle della parte III del presente codice.

3-bis. I Comuni con popolazione non superiore a 5.000 abitanti ricadenti nel territorio di ciascuna Provincia affidano obbligatoriamente ad un'unica centrale di committenza l'acquisizione di lavori, servizi e forniture nell'ambito delle unioni dei comuni, di cui all'articolo 32 del testo unico di cui al decreto legislativo 18 agosto 2000, n. 267, ove esistenti, ovvero costituendo un apposito accordo consortile tra i comuni medesimi e avvalendosi dei competenti uffici. In alternativa, gli stessi Comuni possono effettuare i propri acquisti attraverso gli strumenti elettronici di acquisto gestiti da altre centrali di committenza di riferimento, ivi comprese le convenzioni di cui all'articolo 26 della L. 23 dicembre 1999, n. 488, e il mercato elettronico della PA di cui all'articolo 328 del decreto del Presidente della Repubblica 5 ottobre 2010, n. 207.

La Legge sulla "spending review"

Fra i provvedimenti normativi che le Amministrazioni devono osservare più in generale nelle attività di acquisizione dei beni e servizi e quindi quando debbano dotarsi dei servizi e forniture necessari all'attuazione delle soluzioni di CO/DR, si deve segnalare la legge n. 135 del 2012 di "*Conversione in legge con modificazioni del decreto legge 6 luglio 2012 n. 95: Disposizioni urgenti per la revisione della spesa pubblica con invarianza dei servizi ai cittadini..*" meglio nota anche come "Legge sulla spending review".

La L. n. 135 /2012 da ultimo citata prevede fra l'altro:
art. 1 Riduzione della spesa per l'acquisto di beni e servizi e trasparenza delle procedure
1. Successivamente alla data di entrata in vigore della L. di conversione del presente decreto, i contratti stipulati in violazione dell'articolo 26, c. 3 della L. 23 dicembre 1999, n. 488 ed i contratti stipulati in violazione degli obblighi di approvvigionarsi attraverso gli strumenti di acquisto messi a disposizione da Consip S.p.A. sono nulli, costituiscono illecito disciplinare e sono causa di responsabilità amministrativa. Ai fini della determinazione del danno erariale si tiene anche conto della differenza tra il prezzo, ove indicato, dei detti strumenti di acquisto e quello indicato nel contratto. Le centrali di acquisto regionali, pur tenendo conto dei parametri di qualità e di prezzo degli strumenti di acquisto messi a disposizione da Consip S.p.A., non sono soggette all'applicazione dell'articolo 26, c. 3, della L. 23 dicembre 1999, n. 488. La disposizione del primo periodo del presente comma non si applica alle Amministrazioni dello Stato quando il contratto sia stato stipulato ad un prezzo più basso di quello derivante dal rispetto dei parametri di qualità e di prezzo degli strumenti di acquisto messi a disposizione da Consip S.p.a ed a condizione che tra l'amministrazione interessata e l'impresa non siano insorte contestazioni sulla esecuzione di eventuali contratti stipulati in precedenza
……..
3. Le Amministrazioni pubbliche obbligate sulla base di specifica normativa ad approvvigionarsi attraverso le convenzioni di cui all'articolo 26, c. 3 della L. 23 dicembre 1999, n. 488 stipulate da Consip S.p.A. o dalle centrali di committenza regionali costituite ai sensi dell'articolo 1, c. 455, della L. 27 dicembre 2006, n. 296 possono procedere, qualora la convenzione non sia ancora disponibile e in caso di motivata urgenza, allo svolgimento di autonome procedure di acquisto dirette alla stipula di contratti aventi durata e misura strettamente necessaria e sottoposti a condizione risolutiva nel caso di disponibilità della detta convenzione.
4. Al c. 3-bis dell'articolo 33 del decreto legislativo 12 aprile 2006, n. 163 è aggiunto infine il seguente periodo: "In alternativa, gli stessi Comuni possono effettuare i propri acquisti attraverso gli strumenti elettronici di acquisto gestiti da altre centrali di committenza di riferimento, ivi comprese le convenzioni di cui all'articolo 26 della L. 23 dicembre 1999, n. 488, e il mercato elettronico della PA di cui all'articolo 328 del d.P.R. 5 ottobre 2010, n. 207".
5. (……)
6. Nell'ambito del Mercato elettronico della PA realizzato dal Ministero dell'economia e delle finanze avvalendosi di Consip S.p.A. possono essere istituite specifiche sezioni ad uso delle Amministrazioni pubbliche che, a tal fine, stipulino appositi accordi con il Ministero dell'economia e delle finanze e con Consip S.p.A.

Successivamente la norma prevede al comma 7 che le Amministrazioni sono tenute ad approvvigionarsi attraverso le convenzioni o gli accordi quadro messi a disposizione da Consip S.p.A. e dalle centrali di committenza regionali di riferimento *(articolo 1, c. 455, della L. 27 dicembre 2006, n. 296)* ovvero ad esperire proprie autonome procedure nel rispetto della normativa vigente, utilizzando i sistemi telematici di negoziazione sul mercato elettronico e sul sistema dinamico di acquisizione.

E' fatta salva la possibilità di procedere ad affidamenti, al di fuori delle predette modalità, a condizione che gli stessi conseguano ad approvvigionamenti da altre centrali di committenza o a procedure di evidenza pubblica, e prevedano corrispettivi inferiori a quelli indicati nelle convenzioni e accordi quadro messi a disposizione da Consip S.p.A. e dalle centrali di committenza regionali. In tali casi i contratti dovranno comunque essere sottoposti a condizione risolutiva con possibilità per il contraente di adeguamento ai predetti corrispettivi nel caso di intervenuta disponibilità di convenzioni Consip e delle centrali di committenza regionali che prevedano condizioni di maggior vantaggio economico. La mancata osservanza delle disposizioni del presente c. rileva ai fini della responsabilità disciplinare e per danno erariale.
I contratti stipulati in violazione delle citate disposizioni sono nulli, costituiscono illecito disciplinare e sono causa di responsabilità amministrativa; ai fini della determinazione del danno erariale si tiene anche conto della differenza tra il prezzo, ove indicato, degli strumenti di acquisto citati e di quello indicato nel contratto.

Si prevede anche che:
- l'aggiudicatario delle convenzioni stipulate da Consip S.p.A. e dalle centrali di committenza regionali possa offrire a Consip S.p.A. e alle centrali di committenza regionali, nel corso della durata della rispettiva convenzione e dei relativi contratti attuativi, una riduzione delle condizioni economiche previste nella convenzione che troverà applicazione nei relativi contratti attuativi stipulati e stipulandi a far data da apposita comunicazione che Consip S.p.A. e le centrali di committenza pubblicano sui relativi portali previa verifica dell'effettiva riduzione.
- le Amministrazioni pubbliche che abbiano validamente stipulato un contratto di fornitura o di servizi hanno diritto di recedere in qualsiasi tempo dal contratto (previa formale comunicazione e previo pagamento delle prestazioni già eseguite oltre al decimo delle prestazioni non ancora eseguite), nel caso in cui, tenuto conto anche dell'importo dovuto per le prestazioni non ancora eseguite, i parametri delle convenzioni stipulate da Consip successivamente alla stipula del predetto contratto siano migliorativi rispetto a quelli del contratto stipulato e l'appaltatore non acconsenta ad una modifica, proposta da Consip delle condizioni economiche;
- il diritto di recesso va inserito automaticamente nei contratti in corso ai sensi dell'articolo 1339 c.c., anche in deroga alle eventuali clausole difformi apposte dalle parti;
- Consip e le centrali di committenza regionali, in caso di esercizio del diritto di recesso, possono stipulare una convenzione di cui all'articolo 26 della L. 23 dicembre 1999, n. 488, avente durata fino al 30 giugno 2013, interpellando progressivamente gli operatori economici fino al terzo miglior offerente nelle originarie procedure, a condizione che siano offerte condizioni economiche migliorative tali da determinare il raggiungimento del punteggio complessivo attribuito.

La "*Nota di Aggiornamento del Documento di economia e Finanza 2012*" presentata dal Presidente del Consiglio dei Ministri e dal Ministro dell'Economia e delle Finanze capitolo "4.2 Processo di revisione della spesa" riporta tra l'altro la seguente considerazione: "…*Dal lato della spesa, le misure correttive riguardano la voce relativa all'acquisto di beni e servizi delle Amministrazioni pubbliche con il rafforzamento del sistema centralizzato degli acquisti per alcune categorie merceologiche (attraverso Consip S.p.a. o le centrali di committenza regionali), nonché la nullità dei contratti stipulati in violazione di questo obbligo. I benchmark di spesa per le Amministrazioni pubbliche, e i conseguenti risparmi, sono calcolati sulla base del confronto statistico dei costi di gestione attualmente sostenuti dai diversi enti*…."

Il dialogo competitivo

Il «dialogo competitivo» è una procedura, prevista dall'art. 58 del D.lgs. n.163/2006 e s.m.i. e dal relativo Regolamento di attuazione, nella quale l'Amministrazione, in caso di appalti particolarmente complessi, avvia un dialogo con le imprese candidate ammesse a tale procedura, al fine di elaborare una o più soluzioni atte a soddisfare le sue necessità e sulla base della quale o delle quali i candidati selezionati saranno invitati a presentare le offerte; Qualsiasi operatore economico può chiedere di partecipare a tale procedura.
L'Amministrazione che intende utilizzare il dialogo competitivo, per dare attuazione all'art. 50bis del CAD, potrà procedere a:

- predisporre il Capitolato Tecnico, sulla base dello SFT o della BIA/RA, illustrando le esigenze e le necessità da soddisfare, avendo cura di indicare le caratteristiche principali del proprio sistema ICT (servizi, applicazioni e dati che intende ricoverare) e i valori di RTO e RPO che intende assicurarsi;
- pubblicare un bando di gara conformemente all'articolo 64 del Codice De Lise per rendere note le necessità o obiettivi del progetto che intende affidare per la realizzazione della soluzione di CO/DR, definendola nel bando stesso o in un documento descrittivo (che costituisce parte integrante del bando);

- definire nel bando i requisiti di ammissione al dialogo competitivo (individuati tra quelli pertinenti previsti dagli articoli da 34 a 46 del Codice De Lise), i criteri di valutazione delle offerte (di cui all'articolo 83, c. 2) e il termine entro il quale gli interessati possono presentare istanza di partecipazione alla procedura;
- avviare la fase di preselezione delle imprese, invitandole a presentare domanda di partecipazione con proposte tecniche (e non economiche);
- avviare con i candidati ammessi un dialogo finalizzato all'individuazione e alla definizione delle soluzioni, degli accordi dei livelli di servizio (SLA) e dei mezzi più idonei a soddisfare necessità o obiettivi dell'Amministrazione;
- dichiarare concluso il dialogo, invitando i partecipanti a presentare le loro offerte finali (tecnico-economiche) in base alla o alle soluzioni presentate e specificate nella fase del dialogo. Le offerte presentate devono contenere tutti gli elementi richiesti e necessari per l'esecuzione del progetto;
- valutare le offerte ricevute sulla base dei criteri di aggiudicazione fissati nel bando di gara o nel documento descrittivo, individuando l'offerta economicamente più vantaggiosa (ai sensi dell'articolo 83);
- invitare l'offerente che risulta aver presentato l'offerta economicamente più vantaggiosa a precisare gli aspetti della sua offerta o a confermare gli impegni in essa figuranti, a condizione che ciò non abbia l'effetto di modificare elementi fondamentali dell'offerta o dell'appalto quale posto in gara, falsare la concorrenza o comportare discriminazioni.

Su richiesta dell'Amministrazione le offerte possono essere chiarite, precisate e perfezionate. Tuttavia tali precisazioni, chiarimenti, perfezionamenti o complementi non possono avere l'effetto di modificare gli elementi fondamentali dell'offerta o dell'appalto quale posto in gara, la cui variazione rischi di falsare la concorrenza o di avere un effetto discriminatorio.

I principi della Strategia Lisbona e il "Green Public Procurement"

Nella fase di acquisizione dei beni e servizi diretti alla realizzazione di una soluzione di Continuità Operativa e di Disaster Recovery è opportuno salvaguardare anche la sostenibilità ambientale, avendo cura quindi di definire processi d'acquisto sostenibili, inserendo nei capitolati di gara, adeguatamente valorizzati, requisiti che siano in linea con i criteri diretti ad assicurare il rispetto dell'ambiente; ciò al fine di tener conto dei principi previsti:

- nell'ambito della strategia "Europa 2020" che succederà alla Strategia di Lisbona per il prossimo decennio e che promuove misure per addivenire ad acquisti sostenibili, fissa- in materia di occupazione, innovazione, istruzione, integrazione sociale e clima/energia – ambiziosi obiettivi da raggiungere entro il 2020, al fine di sostenere azioni concrete sia a livello comunitario che nazionale, rendendo la sostenibilità ambientale uno dei pilastri della competitività europea;
- nell'ambito delle Linee Guida emanate dalla Commissione Europea per la redazione di Piani d'azione nazionali sul Green Public Procurement con l'obiettivo di incoraggiare "*gli Stati membri della Comunità a dotarsi di piani d'azione per l'integrazione delle esigenze ambientali negli appalti pubblici*";
- nella Direttiva 2004/18/CE e quindi nel D. Lgs. 163/2006, ove si prevede in materia di GPP che le specifiche tecniche "*ogniqualvolta sia possibile devono essere definite in modo da tener conto dei criteri di protezione ambientale*" e che quando si procede ad affidamenti con il criterio dell'offerta economicamente più vantaggiosa, il bando di gara stabilisce fra i criteri di valutazione dell'offerta pertinenti alla natura, all'oggetto e alle caratteristiche del contratto, oltre al prezzo, alla qualità e al pregio tecnico, estetico e funzionale, anche "*le caratteristiche ambientali ed il contenimento dei consumi energetici e delle risorse ambientali dell'opera o del prodotto*".

D.2 INDICAZIONI PER L'ELABORAZIONE DELLE CLAUSOLE CONTRATTUALI PER REGOLAMENTARE I SERVIZI E LE SOLUZIONI DI CO/DR

Senza avere la pretesa di essere esaustivi, essendo il mercato in continuo divenire ed essendo anche le scelte connesse alla continuità operativa strettamente legate al contesto di riferimento del Sistema Informativo proprio dell'Amministrazione ed alla relativa tipologia dei dati da salvaguardare, si riportano le componenti più significative delle forniture e servizi che si possono richiedere per l'adozione di una soluzione di CO/DR.

Gli aspetti da regolamentare per l'attuazione di una soluzione di CO/DR, ferma la necessità di contestualizzarli a seconda della soluzione e del contratto da definire, sono di seguito schematicamente descritti nelle linee generali.

Il servizio di copia e allineamento dei dati

Per garantire la continuità operativa è indispensabile che sia assicurata dall'Amministrazione, in proprio ovvero ricorrendo ad un prestatore di servizi ICT, il servizio di copia e allineamento dei dati del Sistema Informativo primario con i dati contenuti nelle copie di backup locali e remote (regolamentando opportunamente il regime di responsabilità fra chi è tenuto a effettuare le copie di backup e chi è tenuto ad assicurare il "restore", ove dette responsabilità siano affidate a soggetti diversi).
Detto servizio andrà ovviamente correttamente rapportato all'entità dei dati da salvare e copiare e potrà essere richiesto, ove l'Amministrazione già non ne disponga, unitamente alla fornitura degli apparati HW e SW per l'attività di copia e salvataggio dei dati.

E' necessario specificare la cadenza temporale del servizio di copia dei dati, tenuto conto del contesto tecnico operativo dell'Amministrazione e dei valori di RPO definiti dalla stessa, nonché l'indicazione delle modalità e del luogo di custodia delle copie di backup.
Le attività svolte dovranno essere rendicontate dal fornitore con la cadenza periodica ritenuta opportuna (giornaliera, settimanale, mensile ecc.) e sulla base dei livelli di servizio e degli obiettivi di RPO attesi, dando anche evidenza dei valori registrati.

L'Amministrazione dovrà assicurare la piena conformità agli obblighi previsti dalla normativa del Codice in materia di protezione dei dati personali e dai provvedimenti del Garante per la protezione dei dati personali, con particolare riferimento alle misure di sicurezza e all'individuazione delle figure dei responsabili, degli incaricati al trattamento e degli Amministratori di sistema, prevedendo anche le necessarie attività di verifica e controllo. Al proposito, si ricorda anche l'importanza di osservare i provvedimenti fra cui il provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministrazione di sistema" del 27 novembre 2008.

L'Amministrazione dovrà contestualizzare la tipologia e le modalità di erogazione del servizio sulla base della soluzione tecnologica adottata e verificare il corretto svolgimento del servizio di copia e allineamento dei dati delle copie di back up rispetto ai dati del S.I. primario.

Al riguardo si può verificare anche l'opportunità di chiedere al fornitore, ove l'Amministrazione non ne disponga, di dotare l'Amministrazione di strumenti automatizzati e che consentano al personale dell'Amministrazione stessa il controllo della congruenza e correttezza dei dati salvati e il monitoraggio del servizio valutando eventualmente l'opportunità di richiedere, unitamente e come parte integrante del servizio l'utilizzo di strumenti di monitoring o la predisposizione di cruscotti o portali per la tracciatura ed il controllo automatizzato.

Il sito alternativo - possibili requisiti dei datacenter e dei siti di DR

Garantirsi un servizio di copia dati con trasferimento in un sito remoto non può definirsi di per sé una soluzione di CO/DR: è, infatti, imprescindibile garantirsi soluzioni per l'utilizzo delle copie dei dati trasferiti e il ripristino dell'operatività del Sistema Informativo primario a fronte di eventi imprevisti, condizioni di emergenza e/o disastri.

Pertanto, le Amministrazioni che intendono dotarsi di soluzioni di CO/DR, devono anche individuare un sito da destinare al ruolo di sito alternativo per il ripristino dell'operatività del primario, o valutare – come si avrà modo di illustrare nel prosieguo - la possibilità di utilizzare un sito in condivisione con altri Enti/Amministrazioni, nonché quella di ricorrere ai fornitori presenti sul mercato per richiedere, a seconda dei casi, la fornitura o la messa a disposizione di un sito alternativo efficiente e, per quanto possibile, moderno e rispondente a caratteristiche e requisiti minimi ben definiti.
Nel merito dei requisiti che un datacenter e un sito di DR dovrebbero poter soddisfare si richiama il capitolo 3 delle presenti Linee Guida e la scheda servizi, richiamata nel capitolo 6, ferma restando l'osservanza delle specifiche tecniche e dei vincoli previsti dalla normativa vigente (fra cui, ad esempio: il D.lgs. 9 aprile 2008, n. 81 di "Attuazione dell'art. 1 della L. 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro" e s.m.i. (fra cui, il D.lgs. n. 106/2009 e la L. n. 10/2011); il D.M. del 22 gennaio 2008 n. 37, il "Regolamento concernente l'attuazione dell'articolo 11 – quaterdecies, c. 13, lett.a) della L. n. 248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici"; il D.M del 16 febbraio 1982 così come modificato dai DM 27/03/85 e 30/10/86, e che attiene all'elenco delle attività soggette al rilascio del certificato di prevenzione incendi (C.P.I) da parte dei VV.FF.; le Norme Tecniche per le diverse attività fra cui il D.P.R. 380/2001 contenete il "Testo unico delle disposizioni legislative e regolamentari in materia edilizia" e s.m.i., le Norme Tecniche Costruzioni 2008 e relative Circolari applicative fra cui in particolare la circolare 2 febbraio 2009, n. 617 contenente le "Istruzioni per l'applicazione delle Nuove norme Tecniche per le costruzioni di cui al D.M. 14 gennaio 2008).

Aspetti da tenere in considerazione quando si deve costruire o scegliere un datacenter sono infatti anche quelli connessi alle concessioni edilizie e ai permessi rilasciati dagli uffici competenti del comune di appartenenza dopo aver analizzato la consistenza del terreno e verificato che non vi siano vincoli alla eventuale costruzione. Risulta inoltre importante tener conto dei regolamenti edilizi, degli standard relativi ai controlli sui fabbricati, e di tutti i regolamenti, locali, regionali e statali potenzialmente applicabili.

I regolamenti cambiano anche sensibilmente da città a città e da regione a regione e possono riguardare ogni aspetto della gestione di un datacenter, come per esempio le ore nell'arco di un anno entro cui si può tenere operativo un generatore di emergenza, oppure il periodo della giornata entro cui i camion possono circolare. La conoscenza delle restrizioni esistenti permette di scegliere il sito in maniera adeguata e prepararsi anticipatamente a possibili problematiche regolamentari.
In appendice D al presente documento si riportano a titolo esemplificativo i requisiti che un sito di DR dovrebbe poter soddisfare, tenuto conto dello stato dell'arte dei moderni datacenter e degli standard al riguardo, al fine di ospitare i servizi di DR.

E' ovviamente rimessa alla valutazione discrezionale dell'Amministrazione, in caso di procedura concorsuale, l'individuazione dei requisiti che sono considerati requisiti minimi di partecipazione e di quelli che invece assumono la valenza di specifiche e obblighi di carattere generale ai fini del servizio. I requisiti individuati dall'Amministrazione ai fini della soluzione di CO/DR scelta dovranno essere mantenuti, controllati e verificati, anche in occasione dei test periodici di verifica della costante adeguatezza della soluzione di CO/DR, per tutto il periodo di erogazione dei servizi.

Possibili accorgimenti da richiedere in merito alla disponibilità, gestione e manutenzione di un sito di DR

Come si è già in parte anticipato nei punti precedenti, il fornitore è tenuto a garantire che sia il sito che gli impianti siano stati progettati tenendo conto delle esigenze di continuità e manutenibilità dei moderni datacenter, garantendo per tutto l'arco temporale che lo impegna nei confronti dell'Amministrazione che abbia richiesto la fornitura ovvero la messa a disposizione del sito alternativo di DR:

- l'assoluta sicurezza del sito, ossia l'adozione di soluzioni in linea con lo stato dell'arte, dell'evoluzione tecnologica e della normativa vigente al riguardo, assicurando la protezione da accessi non autorizzati, la presenza di gruppi di continuità e accorgimenti che garantiscano l'erogazione dell'elettricità senza interruzioni, la presenza di dispositivi antincendio e antiallagamento nonché il rispetto dei requisiti richiesti dall'Amministrazione;

- la *fault tolerance* (letteralmente tolleranza ai guasti) con possibilità di isolare l'apparato in fault e provvedere alle riparazioni e/o alla sostituzione delle componenti guaste, senza pregiudicare la continuità delle funzionalità e del servizio erogato;
- la disponibilità a soddisfare le eventuali esigenze di crescita che fosse necessario fronteggiare nel corso dell'erogazione dei servizi di DR.

L'Amministrazione dovrebbe anche esplicitare che il fornitore si impegna a predisporre le opportune misure di protezione fisica per proteggere i dati, contenuti negli apparati storage dedicati alla soluzione di DR, da accessi non autorizzati (fermo restando che rimane a carico dell'Amministrazione la definizione delle politiche di sicurezza per l'accesso applicativo dei dati).
Il fornitore dovrà altresì, per tutto l'arco temporale che lo impegna nei confronti dell'Amministrazione che abbia richiesto la fornitura/la messa a disposizione del sito alternativo di DR, assicurare l'accesso allo stesso sito al personale dell'Amministrazione per consentire, la verifica della costante adeguatezza del sito alla soluzione di DR richiesta e il riscontro del rispetto dei requisiti definiti ai sensi degli articoli 1662 e 1665 del codice civile.
La verifica del rispetto degli obblighi connessi alla disponibilità gestione e manutenzione del sito è opportuno sia considerata come un presupposto essenziale per il pagamento dei corrispettivi dovuti.
Valutata la gravità delle eventuali non conformità riscontrate le Amministrazioni si possono anche riservare la facoltà di risolvere il contratto.
E' anche opportuno impegnare espressamente il fornitore a garantire, a suo carico, gli interventi e le attività di manutenzione ordinaria, preventiva e correttiva nonché il costante aggiornamento tecnologico delle caratteristiche del sito, senza oneri aggiuntivi per l'Amministrazione, essendo la disponibilità del sito con determinate caratteristiche, un requisito minimo di servizio essenziale alla soluzione di DR.
E' anche utile, in linea con la normativa vigente in tema di appalti (D.lgs. 163/2006 e s.m.i., e relativo regolamento di attuazione) - ove se ne ravvisi la necessità - regolamentare contrattualmente eventuali altre opzioni, varianti o situazioni che comportino cambi evolutivi per esigenze dell'Amministrazione.

Le eventuali clausole da definire ai fini della manutenzione della soluzione di CO/DR

Le Amministrazioni devono assicurarsi anche la manutenzione della soluzione di CO/DR e delle componenti HW, SW e di rete che compongono la c.d. configurazione di emergenza.
Le Amministrazioni possono quindi richiedere al prestatore affidatario dei servizi di CO/DR di:

- garantire i servizi per la riattivazione e il ripristino del sistema informativo primario/di produzione dell'Amministrazione, in presenza di un evento catastrofico, di una condizione di emergenza, di un disastro;
- assicurare la disponibilità delle componenti HW e SW della configurazione di emergenza da garantire all'Amministrazione (vi è da considerare che bisogna eventualmente precisare se si richiede la disponibilità di componenti, ad esempio server o storage, destinate in via esclusiva e senza alcuna forma di condivisione);
- pianificare adeguatamente le attività da svolgere per assicurare il funzionamento della soluzione di DR (tenuto conto del regime di responsabilità e se si operi in un regime di affidamento di servizi all'outsourcer o al fornitore dei solo servizi di DR);
- verificare costantemente nell'erogazione dei servizi la capacita della soluzione di DR di rispondere efficacemente alle situazioni di emergenza;
- verificare con l'Amministrazione il costante allineamento dei servizi, delle risorse, delle componenti HW e SW, delle licenze SW necessarie alla soluzione di DR, rispetto all'evoluzione del sistema informatico, della connettività e della struttura organizzativa dell'Amministrazione;
- supportare l'Amministrazione nel valutare l'adeguatezza degli accorgimenti e delle procedure messe in atto per assicurare il ripristino dell'operatività, in occasione delle verifiche e dei test periodici;
- identificare ed attuare, ove possibile, senza impatti o cambiamenti nelle configurazioni e negli ambienti del sistema informativo primario/di produzione dell'Amministrazione, le eventuali misure di aggiornamento tecnologico, adeguamento e/o miglioramento di cui emergesse la necessità nel corso dell'erogazione dei servizi per assicurare l'aderenza della soluzione di DR;
- supportare l'Amministrazione nel verificare periodicamente la soluzione di DR attraverso lo svolgimento delle previste sessioni di test.

L'Amministrazione dovrà, altresì, disciplinare contrattualmente gli impegni del fornitore di assicurare le attività di manutenzione HW e SW, al fine di assicurarsi, il rispetto dei tempi di risoluzione e ripristino previsti a fronte di malfunzionamenti e anomalie di tutte le componenti messe a disposizione nell'ambito della soluzione di Disaster Recovery), anche eseguendo le necessarie riparazioni e sostituzioni.
La verifica del rispetto degli obblighi connessi alla manutenzione della soluzione di DR e delle componenti della configurazione di emergenza, è opportuno sia considerata come un presupposto necessario per il pagamento dei corrispettivi dovuti.
L'Amministrazione potrà anche, per tener conto della possibile crescita fisiologica del proprio S.I., individuare e regolamentare contrattualmente dei meccanismi che, fermo restando il rispetto della normativa vigente, possano tener conto di eventuali esigenze di incremento ad es. dello spazio di storage; del numero dei server; della capacità computazionale; dei canali di collegamento ecc.ecc.

I test periodici della soluzione

Al fine di verificare la corretta erogazione dei servizi e la costante adeguatezza della soluzione di DR necessario che le Amministrazioni prevedano l'impegno del fornitore a sottoporsi a eseguire test periodici (almeno una volta l'anno) per simulare il funzionamento del sito di DR in caso di disastro del sito primario, al fine di verificare che sia assicurato il corretto ripristino del funzionamento del sistema informativo dell'Amministrazione.
Il fornitore dovrà porre in esser ogni attività di sua competenza e supportare l'Amministrazione nell'effettuare i test periodici previsti per la verifica della corretta funzionalità delle soluzioni adottate per garantire la soluzione di Disaster Recovery del sistema informativo primario dell'Amministrazione e assicurare che i servizi erogati vengano costantemente mantenuti allineati all'evoluzione dell'architettura e dei servizi.
Il fornitore dovrà predisporre il test al fine di simulare una "vera" condizione di emergenza/di indisponibilità prolungata e, al fine di non rischiare di compromettere i dati di produzione per l'effettuazione delle simulazioni, dovrà predisporre copie dei dati ad uso esclusivo della simulazione che saranno cancellate al termine delle prove. L'avvenuta cancellazione di dette copie dei dati sarà verificata in contraddittorio dalle parti nei modi e tempi che saranno indicati.
Il fornitore dovrà porre in esser ogni attività di sua competenza e supportare l'Amministrazione nel verificare e testare le procedure formalizzate per garantire, in condizioni di funzionamento normale del centro primario, le operazioni di allineamento dei due centri (copia remota dei dati, ecc.).
E' opportuno che l'Amministrazione valuti la possibilità di chiedere al fornitore di mettere a disposizione strumenti per facilitare la gestione e la conduzione del test anche da remoto.
Il fornitore, nell'effettuazione dei test periodici di Disaster Recovery dovrà simulare uno scenario che prevede l'indisponibilità di tutte le apparecchiature del sito primario e il ripristino nel sito di DR dell'infrastruttura ICT necessaria al riavvio del sistema informativo colpito dalla situazione di emergenza/disastro.
Il test dovrà essere convocato dal fornitore con apposita comunicazione inviata all'Amministrazione (salva restando la possibilità - ove previsto nel contratto relativo - che, invece spetti all'Amministrazione chiedere o concordare con il fornitore, la convocazione del test).
Il test potrà essere articolato secondo le seguenti macro fasi, da definire operativamente nella documentazione annessa al Piano di DR:

- messa a disposizione e verifica di tutta la documentazione procedurale e tecnica connessa ai servizi di DR;
- attivazione e ripartenza dei sistemi nel sito di DR;
- verifica delle funzionalità di base degli ambienti elaborativi;
- verifica dell'allineamento e della congruità dei dati tra il sito primario di produzione e il sito di DR;
- verifica dell'operatività dell'infrastruttura di rete;
- verifica della corretta distribuzione delle rotte IP tra gli apparati di rete;
- verifica connettività tra il sito di DR e i siti primari;
- attivazione dei sottosistemi applicativi;
- test applicativi.

In generale l'attivazione dei sistemi nel sito di DR sarà basata su di una copia aggiuntiva dei volumi a disco da realizzare tramite le funzionalità di copia istantanea dei sottosistemi storage (c.d. flash copy); ciò al fine di permettere l'effettuazione di test su copie aggiuntive dei dati (c.d. "dati a perdere") senza alterare i dati presenti sui volumi a disco costantemente allineati con quelli di produzione localizzati.
Ciò permetterà di effettuare i test senza mai sospendere le sessioni di copia remota e quindi senza abbassare il livello di protezione della soluzione.
Al fine di verificare la rispondenza delle caratteristiche di affidabilità delle infrastrutture del datacenter espressamente richieste come requisiti di partecipazione e capacità tecnica, duranti i test si potrà richiedere la simulazione della indisponibilità dell'infrastruttura tecnologica.
E' opportuno al termine del test prevedere l'obbligo del fornitore di redigere e sottoporre all'accettazione dell'Amministrazione il verbale del test e il documento di tracciatura dell'esito delle prove effettuate.
L'accettazione/approvazione degli esiti del test è necessario sia considerata un presupposto essenziale ai fini del pagamento dei corrispettivi dovuti; è opportuno anche prevedere le penalità in caso di esito negativo e i termini e le modalità per la ripetizione del test, impegnando il fornitore a svolgere ogni attività necessaria per risolvere i problemi evidenziati, restando a suo carico ogni onere derivante dalle attività da porre in essere per risolvere i problemi evidenziati, di sua responsabilità (che non hanno reso possibile concludere con esito positivo il test).

Il servizio di assistenza operativa

L'Amministrazione, ove lo ritenga necessario, può richiedere al fornitore assicurare per tutta la durata del contratto, un servizio di assistenza operativa al fine di garantirsi la presenza di un adeguato supporto e il presidio, la gestione e la manutenzione delle soluzioni adottate.
A tal fine l'Amministrazione può riservarsi di richiedere al fornitore di provvedere ad assicurare la presenza di idoneo e qualificato personale a presidio dell'infrastruttura e delle apparecchiature dedicate alla soluzione di Disaster Recovery garantendo (a titolo esemplificativo e non esaustivo):

- il presidio, la gestione e la manutenzione delle infrastrutture dedicate alla soluzione di Disaster Recovery;
- la manutenzione della soluzione realizzata;
- l'assistenza operativa in condizioni normali e di emergenza e durante l'esecuzione dei test periodici previsti per la verifica del corretto funzionamento delle procedure di DR e del corretto dimensionamento delle componenti connesse alla soluzione di Disaster Recovery;
- il monitoraggio e la gestione delle risorse al fine di mantenere e ottimizzare i livelli di servizio;
- la verifica del costante allineamento fra le copie dei dati del sito di Disaster Recovery e i dati del sistema informativo primario;
- la rendicontazione (che può essere richiesta a seconda delle esigenze dell'Amministrazione con cadenza giornaliera, settimanale, mensile, trimestrale ecc.) dei livelli RPO riscontrati;
- la definizione e il costante adeguamento delle procedure di Disaster Recovery;
- la disponibilità della configurazione di ripristino in caso di emergenza in accordo con i livelli di servizio;
- la predisposizione e l'aggiornamento del Piano di Disaster Recovery nonché della relativa documentazione e manualistica;
- il supporto e l'assistenza per assicurare il ripristino della normalità dalla condizione di emergenza e la ripresa dell'operatività del Sistema Informativo Primario;
- le attività per riportare i dati e le configurazioni dei sistemi dal sito di DR, al sito primario, secondo quanto previsto nel Piano di Disaster Recovery.

Il fornitore avrà il compito di assicurare il corretto funzionamento dei sistemi installati presso il sito di DR sia quando il sito primario dell'Amministrazione opera in condizioni di normale operatività sia per garantirne l'effettiva disponibilità durante le fasi di test e in condizioni di emergenza.
Il servizio di assistenza operativa deve comprendere essenzialmente le attività di presidio per la gestione operativa di tutti i sistemi ospitati nel sito di Disaster Recovery.

Il servizio si può richiedere 7 giorni su 7, 24 ore al giorno, ovvero nelle finestre temporali che l'Amministrazione riterrà sufficienti in considerazione della soluzione scelta.

Durante il periodo di emergenza, il fornitore dovrà assicurare l'assistenza operativa ed il presidio a supporto del personale dell'Amministrazione, che è comunque responsabile della conduzione in esercizio dei sistemi, eventualmente anche tenuto conto, ove richiesto, dello skill e del mix di risorse professionali che l'Amministrazione stessa avrà richiesto e stabilito, in considerazione del dimensionamento effettuato**.**
Possono in questo ambito essere richieste anche le attività per garantire il controllo del corretto funzionamento della configurazione di Disaster Recovery nonché le funzionalità di monitoraggio e gestione degli allarmi relativi:

- alle risorse HW e SW di base dei sistemi (dischi, memoria, processori, connessione di rete, SAN Fabric, …) connessi alla soluzione di DR adottata;
- allo stato dei prodotti di gestione del mirroring e backup;
- alla connettività tra i sistemi del sito primario e del sito di DR.
- il monitoraggio di tutte le funzionalità di mirroring;
- la pianificazione operativa delle attività schedulabili;
- la gestione delle risorse di sistema al fine di mantenere e ottimizzare i livelli di servizio;
- la fornitura dei deliverable e rendicontazioni previste.

Suggerimenti di strumenti, clausole e disposizioni di Carattere Generale

E' necessario prevedere almeno le clausole:

- che regolino l'obbligo di riservatezza e gli obblighi del fornitore di improntare il proprio operato a quanto previsto dal D.lgs. 196/2003 e s.m.i. "Codice in materia di protezione dei dati personali", in particolare, individuando esplicitamente, ai sensi del Titolo IV della parte I del citato codice, le figure che nell'ambito dei servizi richiesti svolgono il ruolo e i compiti di responsabili ed incaricati del trattamento, nonché gli amministratori di sistema, in linea con quanto previsto dalla normativa e dai provvedimenti del Garante per la protezione dei dati personali, personalizzato anche sulla base delle misure di sicurezza dell'Amministrazione; al proposito, si ricorda anche l'importanza di tenere conto dei provvedimenti emessi dal Garante (fra cui come già detto nelle precedenti Linee Guida e nelle presenti il provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministrazione di sistema" del 27 novembre 2008 e i provvedimenti ad esso connessi);
- che prevedano la responsabilità del fornitore qualora nell'adozione delle soluzioni o nella prestazione dei servizi adotti comportamenti in violazione dei diritti di brevetto, di autore e di ogni privativa altrui;
- che impegnino il fornitore al rispetto delle disposizioni vigenti in materia di lavoro, e dei contratti collettivi nonché la normativa in tema di igiene e sicurezza, la normativa previdenziale e antinfortunistica (fra cui il D.lgs. n. 81 e s.m.i.);
- che regolano i casi per addivenire ad un recesso per giusta causa, nonché per regolare la possibilità di recesso, senza necessità di motivare tale decisione, dandone comunicazione scritta alle altre parti, prevedendo eventualmente un periodo di preavviso prima del recesso, salvo l'art. 1671 del c.c.;
- che regolano la riservatezza delle informazioni e le condizioni di non divulgazione, quali ad esempio quelle di seguito riportate:

  1. La Società, preso atto delle particolari esigenze di riservatezza e sicurezza che connotano le prestazioni di cui al presente contratto, dichiara che le informazioni di cui verrà a conoscenza il personale impiegato nella esecuzione del contratto sono coperte da segreto d'ufficio ovvero riservate e si impegna ad assicurare la massima riservatezza interna ed esterna alle attività condotte in collaborazione con l?Amministrazione, apprestando ogni più idoneo presidio organizzativo al fine di impedire qualsiasi tipo di scambio improprio di informazioni all'interno o all'esterno della Società stessa.

  2. La Società si impegna inoltre a vigilare affinché i collaboratori a qualsiasi titolo incaricati di effettuare le prestazioni contrattuali mantengano riservati i dati, le notizie e le informazioni di cui vengano in possesso, non le divulghino né le utilizzino in alcun modo - direttamente o indirettamente - anche dopo il termine del periodo di collaborazione.

  3. A tal fine i supporti di memorizzazione forniti dall'Amministrazione per consentire ricerche ed analisi di malfunzionamenti relativi ai prodotti messi a disposizione dalla Società, devono essere custoditi dalla Società stessa con la massima cura, non ne devono essere fatte duplicazioni e devono essere restituiti all'Amministrazione al termine delle attività.

4. Del pari, eventuali tabulati ricavati da elaborazioni dei cennati supporti ovvero stampe degli stessi dovranno essere custoditi con la massima cura, distrutti subito dopo l'utilizzo e non dovranno essere oggetto di copia, né totale, né parziale.
5. L'Amministrazione riterrà la Società responsabile di ogni utilizzo improprio delle informazioni sopra cennate, ad essa o ai suoi dipendenti ascrivibile.
6. La Società dovrà inoltre far pervenire all'Amministrazione la dichiarazione allegato "x", sottoscritta dal proprio legale rappresentante.
7. La Società si impegna a far sottoscrivere, da ciascuno degli elementi impegnati nelle attività di esecuzione del presente contratto, la dichiarazione allegato "x"; dette dichiarazioni devono essere custodite dalla Società e prontamente esibite alla Banca su sua richiesta motivata.
8. È vietato alla Società di pubblicizzare, nell'interesse proprio o di terzi, le prestazioni effettuate a favore dell'Amministrazione.
9. L'Amministrazione, a suo insindacabile giudizio, potrà consentire deroghe a tale divieto mediante rilascio di autorizzazione scritta.

Si rammenta che le Amministrazioni, oltre ad inserire le clausole che definiscono le modalità di collaudo della soluzione e di verifica di conformità dei servizi sia all'avvio di un progetto sia durante l'erogazione dei servizi di DR affidati, devono chiarire le modalità di verifica e pagamento dei servizi e forniture ad. es. esplicitando nel contratto che si procederà al pagamento:

- in via posticipata, previa verifica del corretto svolgimento del servizio, precisando se il pagamento avverrà a canone o sulla base del "consumo" tenuto conto dello svolgimento dei test o della durata del periodo di permanenza presso il sito di DR ecc.;
- la cadenza (mensile, trimestrale ecc.) e i presupposti che rendono possibile procedere al pagamento dei corrispettivi dovuti.

Si rammenta di definire le clausole contrattuali al fine di prevedere termini di fatturazione e pagamento in linea con i termini previsti dal D.lgs. n. 231/01 e dalla Direttiva Comunitaria relativa, definendo anche quanto previsto dalla L. 136/2006, così come modificata dal D.L. del 12 novembre 2010, n. 187 in materia di tracciabilità dei flussi finanziari e s.m.i. e prevedendo la nullità o risoluzione di diritto a fronte di inadempimenti agli obblighi previsti.

E' opportuno specificare nel contratto che regolerà le prestazioni affidate ai fini della soluzione di DR i livelli di servizio e i risultati attesi, al venir meno dei quali l'Amministrazione si riserva di non procedere all'accettazione dei servizi e al pagamento dei corrispettivi, chiarendo anche, le fattispecie gli obblighi e vincoli richiesti per i servizi e le forniture che in caso di inadempimento possono dar luogo all'applicazione di penalità, all'esercizio della facoltà di risoluzione e alle azioni di risarcimento danni.
E' necessario poi subordinare l'efficacia del contratto e gli obblighi dell'Amministrazione al rispetto da parte del fornitore della legislazione antimafia prevedendo specifiche clausole nelle quali si definisca la risoluzione di diritto o i casi in cui l'Amministrazione si riserva la facoltà di dichiarare risolto il contratto.

D.3 INDICAZIONI UTILI QUALORA SI ADOTTINO SOLUZIONI "CLOUD".

Come si è già avuto modo di evidenziare nelle presenti Linee Guida, in particolar modo nel capitolo 6, ove si adottino soluzioni cloud una notevole mole di dati può trovarsi a transitare e/o risiedere all'estero, spesso in luoghi diversi e non conosciuti né conoscibili al titolare dei dati.

Si ricorda che il Codice in materia di protezione dei dati personali (D.lgs.196/2003 e s.m.i., in particolare come innovato dal D.lgs. n. 69 del 28 maggio 2012), oltre a regolare i diritti dell'interessato, a prevedere gli obblighi di acquisizione del consenso dell'interessato e di informativa, a disciplinare i ruoli e compiti dei soggetti che effettuano il trattamento (il titolare, il responsabile, gli incaricati) e gli adempimenti e le misure per garantire la corretta gestione e trattamento dei dati (soprattutto quelli sensibili) e la sicurezza dei dati e dei sistemi, nel Titolo VII della parte I che regola il "Trasferimento dei dati all'estero".

Nel Titolo citato si prevede quanto segue:

Art. 42. Trasferimenti all'interno dell'Unione europea

1. Le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

Art. 43. Trasferimenti consentiti in Paesi terzi

1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando:

a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta;

b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con Legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21;

d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, c. 2;

e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla L. 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, c. 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;

Art. 44. Altri trasferimenti consentiti

1. Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

a) individuate dal Garante anche in relazione a garanzie prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo. L'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice, anche in ordine all'inosservanza delle garanzie medesime;

b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

Art. 45. Trasferimenti vietati
1. Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

La tematica è seguita con attenzione dal Garante per la protezione dei dati personali concentrando, da un lato, la propria attività, anche ispettiva, sul settore del cloud computing (vedere newsletter del garante del 4 febbraio 2011 e i vari provvedimenti e raccomandazioni emessi (e già citati nelle presenti Linee Guida), dall'altro sottolineando le proprie perplessità in relazione a questa tecnologia ed evidenziando l'obsolescenza della normativa attualmente vigente rispetto al mutato scenario tecnologico.
Per la verifica della coerenza delle soluzioni cloud rispetto alle indicazioni e suggerimenti forniti nelle presenti Linee Guida e nei documenti in esse richiamati, si potrà utilizzare la seguente cheklist:

ELEMENTO DA VERIFICARE	**coerente/ non coerente -**
Servizio di copia e allineamento dei dati	
E' indispensabile che sia assicurata dall'Amministrazione, in proprio ovvero ricorrendo ad un prestatore di servizi ICT, **il servizio di copia e allineamento dei dati del Sistema Informativo primario** con i dati contenuti nelle copie di backup locali e remote	
E' necessario **specificare la cadenza temporale** del servizio di copia dei dati, tenuto conto del contesto tecnico operativo dell'Amministrazione e dei valori di RPO definiti dalla stessa, nonché l'indicazione delle modalità e del luogo di custodia delle copie di backup.	
Le attività svolte dovranno essere rendicontate dal fornitore con la cadenza periodica ritenuta opportuna (giornaliera, settimanale, mensile ecc.) e sulla base dei livelli di servizio e degli obiettivi di RPO attesi, dando anche evidenza dei valori registrati.	
L'Amministrazione dovrà assicurare la **piena conformità agli obblighi previsti dalla normativa del Codice in materia di protezione dei dati personali** e dai provvedimenti del garante, con particolare riferimento alle misure di sicurezza e all'individuazione delle figure dei responsabili, degli incaricati al trattamento e degli Amministratori di sistema, prevedendo anche le necessarie attività di verifica e controllo.	
L'Amministrazione dovrà **verificare il corretto svolgimento del servizio di copia e allineamento dei dati delle copie di back up rispetto ai dati del S.I. Primario**. Al riguardo si può verificare anche l'opportunità di chiedere al fornitore, ove l'Amministrazione non ne disponga, di dotare l'Amministrazione di strumenti automatizzati e che consentano al personale dell'Amministrazione stessa il controllo della congruenza e correttezza dei dati salvati e il monitoraggio del servizio valutando eventualmente l'opportunità di richiedere, unitamente e come parte integrante del servizio l'utilizzo di strumenti di monitoring o la predisposizione di cruscotti o portali per la tracciatura ed il controllo automatizzato	
Possibili requisiti dei datacenter e dei siti di DR	
Le Amministrazioni che intendono dotarsi di soluzioni di CO/DR, devono anche **individuare un sito da destinare al ruolo di sito alternativo** per il ripristino dell'operatività del primario	
Nel merito dei requisiti che un datacenter e un sito di DR dovrebbero poter soddisfare si richiama **l'osservanza delle specifiche tecniche e dei vincoli previsti dalla normativa vigente** (fra cui, ad esempio: il D.lgs. 9 aprile 2008, n. 81 di "Attuazione dell'art. 1 della	

ELEMENTO DA VERIFICARE	coerente/ non coerente -
Legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro" e s.m.i. (fra cui, il D.lgs. n. 106/2009 e la legge n. 10/2011); il D.M. del 22 gennaio 2008 n. 37, il "Regolamento concernente l'attuazione dell'articolo 11 – quaterdecies, c. 13, lett.a) della legge n. 248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici"; il D.M del 16 febbraio 1982 così come modificato dai DM 27/03/85 e 30/10/86, e che attiene all'elenco delle attività soggette al rilascio del certificato di prevenzione incendi (C.P.I) da parte dei VV.FF.; le Norme Tecniche per le diverse attività fra cui il D.P.R. 380/2001 contenete il "Testo unico delle disposizioni legislative e regolamentari in materia edilizia" e s.m.i., le Norme Tecniche Costruzioni 2008 e relative Circolari applicative fra cui in particolare la circolare 2 febbraio 2009, n. 617 contenente le "Istruzioni per l'applicazione delle Nuove norme Tecniche per le costruzioni di cui al D.M. 14 gennaio 2008).	
Possibili servizi da richiedere in merito alla disponibilità, gestione e manutenzione di un sito di DR	
Il fornitore è tenuto a **garantire l'assoluta sicurezza del sito**, ossia l'adozione di soluzioni in linea con lo stato dell'arte, dell'evoluzione tecnologica e della normativa vigente al riguardo, assicurando la **protezione da accessi non autorizzati**, la presenza di **gruppi di continuità** e accorgimenti che garantiscano l'erogazione dell'elettricità senza interruzioni, la presenza di **dispositivi antincendio e antiallagamento** nonché il rispetto dei requisiti richiesti dall'Amministrazione	
Il fornitore è tenuto a **garantire la *fault tolerance*** (letteralmente tolleranza ai guasti) con possibilità di isolare l'apparato in fault e provvedere alle riparazioni e/o alla sostituzione delle componenti guaste, senza pregiudicare la continuità delle funzionalità e del servizio erogato	
Il fornitore è tenuto a garantire la disponibilità a **soddisfare le eventuali esigenze di crescita** che fosse necessario fronteggiare nel corso dell'erogazione dei servizi di DR.	
L'Amministrazione dovrebbe anche esplicitare che il fornitore si impegna a predisporre le **opportune misure di protezione fisica per proteggere i dati, contenuti negli apparati storage dedicati alla soluzione di DR**, da accessi non autorizzati (fermo restando che rimane a carico dell'Amministrazione la definizione delle politiche di sicurezza per l'accesso applicativo dei dati).	
Il fornitore dovrà altresì, per tutto l'arco temporale che lo impegna nei confronti dell'Amministrazione che abbia richiesto la fornitura/la messa a disposizione del sito alternativo di DR, **assicurare l'accesso allo stesso sito al personale dell'Amministrazione** per consentire, la verifica della costante adeguatezza del sito alla soluzione di DR richiesta e il riscontro del rispetto dei requisiti definiti ai sensi degli articoli 1662 e 1665 del codice civile.	
E' anche opportuno impegnare espressamente il fornitore a **garantire**, a suo carico, **gli interventi e le attività di manutenzione ordinaria, preventiva e correttiva nonché il costante aggiornamento tecnologico delle caratteristiche del sito**, senza oneri aggiuntivi per l'Amministrazione, essendo la disponibilità del sito con determinate caratteristiche, un requisito minimo di servizio essenziale alla soluzione di DR.	
Le eventuali prestazioni da richiedere ai fini della manutenzione della soluzione di CO/DR	
Le Amministrazioni possono richiedere al prestatore affidatario dei servizi di CO/DR di **garantire i servizi per la riattivazione e il ripristino del sistema informativo primario/di produzione dell'Amministrazione, in presenza di un evento catastrofico**, di una condizione di emergenza, di un disastro	
Le Amministrazioni possono richiedere al prestatore affidatario dei servizi di CO/DR di **assicurare la disponibilità delle componenti HW e SW della configurazione di emergenza** da garantire all'Amministrazione (vi è da considerare che bisogna eventualmente precisare se si richiede la disponibilità di componenti, ad esempio server o storage, destinate in via esclusiva e senza alcuna forma di condivisione);	

ELEMENTO DA VERIFICARE	coerente/ non coerente -
Le Amministrazioni possono richiedere al prestatore affidatario dei servizi di CO/DR di **pianificare adeguatamente le attività da svolgere per assicurare il funzionamento della soluzione di DR**	
Le Amministrazioni possono richiedere al prestatore affidatario dei servizi di CO/DR di verificare costantemente nell'erogazione dei servizi la capacita della soluzione di DR di **rispondere efficacemente alle situazioni di emergenza**	
Le Amministrazioni possono richiedere al prestatore affidatario dei servizi di CO/DR di verificare con l'Amministrazione il **costante allineamento dei servizi, delle risorse, delle componenti HW e SW, delle licenze SW necessarie alla soluzione di DR**, rispetto all'evoluzione del sistema informatico, della connettività e della struttura organizzativa dell'Amministrazione	
Le Amministrazioni possono richiedere al prestatore affidatario dei servizi di CO/DR di identificare ed attuare, ove possibile, senza impatti o cambiamenti nelle configurazioni e negli ambienti del sistema informativo primario/di produzione dell'Amministrazione, le eventuali **misure di aggiornamento tecnologico, adeguamento e/o miglioramento** di cui emergesse la necessità nel corso dell'erogazione dei servizi per assicurare l'aderenza della soluzione di DR;	
Le Amministrazioni possono richiedere al prestatore affidatario dei servizi di CO/DR di supportare l'Amministrazione nel verificare periodicamente la soluzione di DR attraverso lo **svolgimento delle previste sessioni di test.**	
L'Amministrazione dovrà, altresì, disciplinare contrattualmente gli impegni del fornitore di **assicurare le attività di manutenzione HW e SW**, al fine di assicurarsi, il rispetto dei tempi di risoluzione e ripristino previsti a fronte di malfunzionamenti e anomalie di tutte le componenti messe a disposizione nell'ambito della soluzione di Disaster Recovery, anche eseguendo le necessarie riparazioni e sostituzioni.	
L'Amministrazione potrà anche, per tener conto della possibile crescita fisiologica del proprio S.I., individuare e regolamentare contrattualmente dei meccanismi che, fermo restando il rispetto della normativa vigente, possano **tener conto di eventuali esigenze di incremento ad es. dello spazio di storage; del numero dei server; della capacità computazionale; dei canali di collegamento ecc.ecc**	
I test periodici della soluzione	
Al fine di verificare la corretta erogazione dei servizi e la costante adeguatezza della soluzione di DR necessario che le Amministrazioni prevedano l'impegno del fornitore a sottoporsi a eseguire **test periodici (almeno una volta l'anno)** per simulare il funzionamento del sito di DR in caso di disastro del sito primario, al fine di verificare che sia assicurato il corretto ripristino del funzionamento del sistema informativo dell'Amministrazione.	
Il fornitore dovrà predisporre il test al fine di simulare una "vera" condizione di emergenza/di indisponibilità prolungata e, **al fine di non rischiare di compromettere i dati di produzione per l'effettuazione delle simulazioni, dovrà predisporre copie dei dati ad uso esclusivo della simulazione che saranno cancellate al termine delle prove.** L'avvenuta cancellazione di dette copie dei dati sarà verificata in contraddittorio dalle parti nei modi e tempi che saranno indicati.	
Il fornitore dovrà porre in esser ogni attività di sua competenza e supportare l'Amministrazione nel verificare e **testare le procedure formalizzate per garantire**, in condizioni di funzionamento normale del centro primario, **le operazioni di allineamento dei due centri (copia remota dei dati, ecc.).**	
E' opportuno che l'Amministrazione valuti la possibilità di chiedere al fornitore di mettere a disposizione strumenti per facilitare la gestione e la **conduzione del test anche da remoto**.	
Il fornitore, nell'effettuazione dei test periodici di Disaster Recovery dovrà **simulare uno scenario che prevede l'indisponibilità di tutte le apparecchiature del sito primario** e il ripristino nel sito di DR dell'infrastruttura ICT	

ELEMENTO DA VERIFICARE	coerente/ non coerente -
Il test **dovrà essere convocato dal fornitore con apposita comunicazione inviata all'Amministrazione** (salva restando la possibilità - ove previsto nel contratto relativo - che, invece spetti all'Amministrazione chiedere o concordare con il fornitore, la convocazione del test).	
Il test potrà essere articolato secondo le seguenti macro fasi, da definire operativamente nella documentazione annessa al Piano di DR: · messa a disposizione e **verifica di tutta la documentazione procedurale** e tecnica connessa ai servizi di DR; · **attivazione e ripartenza dei sistemi nel sito di DR**; · **verifica delle funzionalità di base** degli ambienti elaborativi; · **verifica dell'allineamento e della congruità dei dati** tra il sito primario di produzione e il sito di DR; · **verifica dell'operatività dell'infrastruttura di rete**; · **verifica della corretta distribuzione delle rotte IP** tra gli apparati di rete; · **verifica connettività tra il sito di DR e i siti primar**i; · **attivazione dei sottosistemi applicativi**; · **test applicativi**.	
E' opportuno al termine del test prevedere **l'obbligo del fornitore di redigere e sottoporre all'accettazione dell'Amministrazione il verbale del test** e il documento di tracciatura dell'esito delle prove effettuate.	
Il fornitore si impegna a svolgere ogni attività necessaria per risolvere i problemi evidenziati, restando a suo carico ogni onere derivante dalle attività da porre in essere per risolvere i problemi evidenziati, di sua responsabilità (che non hanno reso possibile concludere con esito positivo il test).	
Il servizio di assistenza operativa	
L'Amministrazione può riservarsi di richiedere al fornitore di provvedere ad assicurare la presenza di **idoneo e qualificato personale a presidio dell'infrastruttura e delle apparecchiature dedicate alla soluzione di Disaster Recovery**	
E' previsto il **monitoraggio e la gestione delle risorse** al fine di mantenere e ottimizzare i livelli di servizio	
E' prevista la definizione e il **costante adeguamento delle procedure di Disaster Recovery**	
E' prevista la verifica del costante **allineamento fra le copie dei dati** del sito di Disaster Recovery e i dati del sistema informativo primario	
E' prevista **la rendicontazione** (che può essere richiesta a seconda delle esigenze dell'Amministrazione con cadenza giornaliera, settimanale, mensile, trimestrale ecc.) **dei livelli RPO riscontrati**	
E' prevista la predisposizione e l'**aggiornamento del Piano di Disaster Recovery nonché della relativa documentazione e manualistica**	
E' prevista l'**assistenza operativa in condizioni normali e di emergenza e durante l'esecuzione dei test periodici previsti** per la verifica del corretto funzionamento delle procedure di DR e del corretto dimensionamento delle componenti connesse alla soluzione di Disaster Recovery	
E' previsto il **supporto e l'assistenza per assicurare il ripristino della normalità dalla condizione di emergenza e la ripresa dell'operatività del Sistema Informativo Primario**	
Sono previste **attività per riportare i dati e le configurazioni dei sistemi dal sito di DR, al sito primario**, secondo quanto previsto nel Piano di Disaster Recovery.	
Il servizio di assistenza operativa si può richiedere 7 giorni su 7, 24 ore al giorno, ovvero nelle **finestre temporali che l'Amministrazione riterrà sufficienti** in considerazione della soluzione scelta.	
Durante il periodo di emergenza, il fornitore dovrà assicurare l'assistenza operativa ed il presidio a supporto del personale dell'Amministrazione, che è comunque responsabile della conduzione in esercizio dei sistemi, eventualmente anche	

ELEMENTO DA VERIFICARE	coerente/ non coerente -
tenuto conto, ove richiesto, dello skill e del mix di risorse professionali che l'Amministrazione stessa avrà richiesto e stabilito, in considerazione del dimensionamento effettuato.	
Possono in questo ambito essere richieste anche le attività per garantire il controllo del corretto funzionamento della configurazione di Disaster Recovery nonché le **funzionalità di monitoraggio e gestione degli allarmi relativi**: · alle risorse HW e SW di base dei sistemi (dischi, memoria, processori, connessione di rete, SAN Fabric, …) connessi alla soluzione di DR adottata; · allo stato dei prodotti di gestione del mirroring e backup; · alla connettività tra i sistemi del sito primario e del sito di DR. · il monitoraggio di tutte le funzionalità di mirroring; · la pianificazione operativa delle attività schedulabili; · la gestione delle risorse di sistema al fine di mantenere e ottimizzare i livelli di servizio; · la fornitura dei deliverable e rendicontazioni previste.	

D.4 INDICAZIONI PER L'ADOZIONE DEL MUTUO SOCCORSO

La dizione "mutuo soccorso" deriva dalle omonime società sorte nella seconda metà dell'800, che offrivano appunto soccorso e aiuti a fronte di calamità e situazioni critiche. Tali soluzioni si caratterizzano – generalmente – per il basso costo e il basso livello di servizio. Sono basate su impegni di assistenza volontaria e non prevedono soluzioni tecniche complesse. Sono particolarmente adatte a fronteggiare situazioni di emergenza particolari, ove sia accettabile la possibilità di un periodo di discontinuità del servizio.
Le organizzazioni che stipulano un accordo di mutuo soccorso si offrono reciprocamente risorse, ospitalità e supporto logistico. Gli accordi possono essere modulati in relazione alle specifiche esigenze, da un semplice impegno d'aiuto sino a veri e propri patti che impegnano le organizzazioni a fornire livelli di assistenza predeterminati.
Generalmente, comunque, l'assistenza fornita all'organizzazione colpita dall'evento critico è "la migliore possibile" (cioè, semplicemente ciò che si può fare con le risorse a disposizione): la soluzione tecnica viene dettagliata nel momento in cui l'evento si manifesta.
Le soluzioni basate su accordi di mutuo soccorso sono tanto più efficaci quanto più sono simili le organizzazioni interessate. In particolare, le condizioni che favoriscono l'efficacia sono:

- comunanza di compiti;
- problematiche di continuità analoghe e non particolarmente stringenti;
- sistemi informativi con dimensioni e architetture simili;
- disponibilità di risorse per situazioni di emergenza (locali, CPU, spazio disco, ecc).

Gli accordi possono essere bilaterali o riguardare più di due organizzazioni. Nel secondo caso, ovviamente, cresce la complessità del piano d'emergenza. In particolare, gli accordi multilaterali devono comprendere un metodo formalizzato per la determinazione del destinatario della richiesta di soccorso: vale a dire, l'accordo deve specificare chiaramente a chi – tra le varie organizzazioni firmatarie – si deve chiedere aiuto nelle varie situazioni critiche; in alternativa, è opportuno che un ente terzo (ad esempio un organismo istituzionale) coordini le attività di soccorso in situazione di emergenza.
Esempio: un accordo di mutuo soccorso può prevedere che l'organizzazione soccorritrice renda disponibili locali attrezzati e apparati ausiliari (alimentazione, LAN, router, PC, ecc.) mentre l'organizzazione in emergenza provvede ad acquisire i server necessari per ripristinare il servizio. Se quest'ultima dispone dei salvataggi dei dati e degli ambienti elaborativi, una volta che si è recuperato l'hardware è possibile ristabilire la configurazione e riattivare il servizio in tempi dell'ordine di 1-2 giorni. Nel caso di accordi tra più organizzazioni con sistemi analoghi, gli apparati necessari per il ripristino possono essere acquisiti anticipatamente con il contributo di tutti gli aderenti all'accordo e conservati in una sede opportuna, per poi essere trasportati all'occorrenza nel sito che ospita l'organizzazione in emergenza. Per gli scopi della PA, è opportuno approfondire due particolari tipologie di accordo di mutuo soccorso, cioè gli accordi tra organizzazioni indipendenti e gli accordi tra strutture di una stessa organizzazione.

Accordi tra organizzazioni indipendenti

Questo tipo di accordo si stipula normalmente quando un'organizzazione dispone di risorse logistiche ed elaborative sovrabbondanti rispetto alle esigenze ordinarie, per cui può ritenere conveniente individuare un partner che si trovi nella stessa condizione e abbia interesse a stipulare un patto di mutua assistenza per fronteggiare situazioni critiche.
Si noti che la condizione di "esubero di risorse", specie nel settore pubblico, si verifica di rado. Inoltre, spesso, la soluzione del mutuo soccorso trova ostacolo nelle esigenze di riservatezza verso organizzazioni estranee[8]. Per questo motivo gli accordi di mutuo soccorso tra organizzazioni indipendenti non sono molto frequenti e, di regola, non coinvolgono più di due organizzazioni.

[8] Infatti in caso di necessità e durante le prove bisogna consentire all'organizzazione ospite di accedere alle proprie strutture informatiche e, benché sia possibile dedicarle ambienti elaborativi isolati, è difficile impedire che essa venga a conoscenza, almeno in parte, di informazioni (organizzazione, strutture, architettura, ecc.) che potrebbero avere un carattere riservato.

L'accordo tipico tra organizzazioni indipendenti è scarsamente vincolante o non lo è affatto: ciascuna organizzazione assisterà l'altra solo a certe condizioni. Potrebbero perciò verificarsi circostanze particolari che impediscono il rispetto degli accordi (ad esempio una situazione di contemporanea emergenza nelle organizzazioni che hanno sottoscritto l'accordo). Questo tipo di accordo può prevedere:

- un impegno generico di assistenza (in questo caso la modalità di soccorso viene determinata al momento di necessità);
- un salvataggio incrociato delle informazioni (ogni organizzazione, ad esempio, può conservare nei propri locali i dischi di backup dell'altra organizzazione) con periodicità fissata;
- un aiuto di tipo logistico (in caso di necessità vengono messi a disposizione locali attrezzati);
- la disponibilità di risorse elaborative e di comunicazione dedicate o condivise;
- la collaborazione del personale per le attività necessarie al ripristino dei servizi.

Gli accordi di mutuo soccorso meno vincolanti possono basarsi su un piano di continuità operativa elementare: in tal caso la cura delle attività di ripristino sarà demandata, al momento dell'emergenza, a un comitato di crisi cui è opportuno partecipino rappresentanti di entrambe le organizzazioni.
In caso di accordo più impegnativo, è opportuno che entrambe le organizzazioni, per rendere più efficaci le attività di ripristino, elaborino un piano di continuità operativa comune, ove siano determinate in anticipo le principali azioni che ciascuna parte compierà in caso di emergenza. In questo caso è consigliabile che le organizzazioni verifichino periodicamente l'efficacia del piano mediante prove congiunte.
Gli accordi tra organizzazioni indipendenti possono essere agevolati grazie al patrocinio di un ente terzo. Quest'ultimo può essere un organismo istituzionale che, per ruolo, promuove e favorisce accordi di mutuo soccorso tra organismi responsabili dell'erogazione di servizi ritenuti fondamentali9. In tal caso, l'ente terzo può essere parte attiva nella definizione dei piani d'emergenza e nel coordinamento delle attività di soccorso.

Accordi tra strutture di una stessa organizzazione

Sono gli accordi di mutua assistenza più frequenti, e vengono stipulati tra più strutture, facenti parte di una medesima organizzazione, che erogano servizi in modo autonomo (ad esempio filiali o sedi periferiche di uno stesso ente, dipartimenti di un'università).
In questo caso, lo schema di accordo potrà essere sviluppato da una struttura centrale, tenendo conto delle esigenze delle strutture che possono essere interessate. Ciascuna struttura potrà decidere se aderire o meno all'accordo; in caso di adesione, dovrà impegnarsi a soccorrere le strutture in condizioni di emergenza offrendo supporto logistico e rendendo disponibile parte delle proprie risorse elaborative10.
L'accordo è quasi sempre di tipo multilaterale: la struttura centrale ha il compito di redigere un modello di PCO e uno schema di accordo che sia valido per tutta l'organizzazione. Ciascuna struttura aderente all'accordo dovrà personalizzare il PCO in funzione delle proprie specificità ed esigenze e dovrà predisporre le risorse occorrenti per eventuali attività di soccorso11. Nel caso in cui un'emergenza coinvolga più strutture, normalmente la struttura centrale svolge il ruolo di coordinamento dei soccorsi.

---

9 Questo ruolo potrebbe essere svolto dalla Protezione civile, a un Ministero o da un'amministrazione periferica.

10 In alcune organizzazioni, l'adesione all'accordo di mutuo soccorso è obbligatoria per tutte le strutture. In questi casi però gli accordi sono quasi sempre di tipo vincolante, dunque le problematiche sono più simili a quelle dell'approccio basato su risorse condivise.

11 A seconda della natura dell'organizzazione, la struttura centrale può avere un ruolo più o meno attivo nel definire le risorse logistiche, strumentali e di personale che ciascuna struttura deve predisporre. In alcuni casi l'accordo può prevedere che le strutture aderenti contribuiscano finanziariamente alla predisposizione di risorse comuni per l'emergenza. La struttura centrale può inoltre fungere da centro di backup centralizzato dei dati presenti nelle strutture che aderiscono all'accordo.

Vantaggi e svantaggi del mutuo soccorso

Come detto, il principale limite di questo tipo di soluzione è il suo approccio "volontaristico". A meno che non si basino su un contratto ben definito, accordi di questo tipo corrono il rischio di non essere onorati e l'organizzazione soccorritrice potrebbe non essere sempre disponibile a prestare assistenza quando occorre.
Chi sceglie una soluzione di mutuo soccorso, dunque, deve poter sopportare tempi di ripristino del servizio variabili anche in modo significativo. Se un'amministrazione ha esigenze di continuità più stringenti, questa soluzione deve essere scartata in favore di soluzioni che
prevedano specifiche risorse (condivise o dedicate) deputate alle attività di ripristino.
Può accadere inoltre che, nel tempo, le due organizzazioni che hanno stretto l'accordo facciano evolvere indipendentemente le proprie infrastrutture, fino a renderle incompatibili. Ancora, potrebbero avvenire dispute tra le due parti, inoltre insorgere questioni di sicurezza, di protezione della proprietà intellettuale e di informazioni confidenziali, tutte problematiche connesse alla natura i questo tipo di soluzione.
Nonostante questi limiti, gli accordi di mutuo soccorso possono rappresentare una valida soluzione in moltissimi casi: numerose Amministrazioni, difatti, non hanno particolari esigenze di continuità operativa, ma devono semplicemente evitare la perdita del patrimonio informativo o l'interruzione prolungata dei servizi. In questi casi, gli accordi di mutua assistenza consentono di evitare queste evenienze con costi ridotti.
Esempi di Amministrazioni che potrebbero trovare adeguata una soluzione di questo tipo sono scuole, musei, biblioteche, ospedali (limitatamente alle risorse dedicate ai sistemi gestionali), in generale Amministrazioni medio-piccole.

Aspetti contrattuali dell'accordo di mutuo soccorso

Di seguito, al fine di fornire una guida alla stipula di un accordo di mutua assistenza, vengono elencati ed illustrati brevemente alcuni elementi tipici di tale tipo di accordo relativo ai servizi informatici.
Si precisa che le clausole dell'accordo dipendono essenzialmente da ciò che viene concordato dalle parti in merito alla tipologia ed i livelli di mutua assistenza. Pertanto le indicazioni che seguono devono essere considerate semplicemente come gli elementi di partenza per discutere, condividere e formalizzare l'accordo vero e proprio.

CLAUSOLE GENERALI

Ambito di applicazione

Definisce il contesto cui l'accordo si riferisce, identificando le organizzazioni, le sedi e le tipologie di attività o servizi. Nel caso l'accordo per la continuità operativa faccia parte di un più ampio accordo di mutua assistenza relativo ad altri settori (energia, tutela del patrimonio artistico, ecc.), è opportuno farne esplicita menzione.
Ad esempio:
"l'accordo si inserisce nel piano di reciproca assistenza di cui al protocollo d'intesa … del … e riguarda la collaborazione per la continuità dei servizi informatici degli enti firmatari di seguito riportati, con riferimento alle sedi operative site sul territorio nazionale.".

Oggetto dell'accordo

Stabilisce i termini dell'accordo. E' opportuno precisare la tipologia di accordo sia per quanto riguarda il tipo di assistenza che ciascuna parte si impegna a fornire, sia relativamente ai servizi cui l'assistenza si riferisce.
Ad esempio:
"ciascuna parte si impegna a fornire la migliore assistenza possibile nel caso l'altra parte si trovi in una circostanza calamitosa che comporti l'interruzione dei servizi informatici essenziali per un periodo di tempo significativo. L'assistenza sarà finalizzata a consentire il ripristino dei servizi informatici essenziali mediante risorse strumentali alternative che saranno approntate all'occorrenza secondo il piano di continuità operativa. La parte soccorritrice renderà disponibili i locali, gli apparati informatici ed i collegamenti telematici, nei limiti delle proprie disponibilità, fatte salve le esigenze di continuità dei propri servizi informatici.".

Impegno economico

Va precisato l'eventuale impegno economico che l'accordo prevede per ciascuna parte.
Di norma questi accordi sono a titolo non oneroso, in tal caso è opportuno inserire una clausola del tipo:

"le parti convengono che i vantaggi derivanti dalla mutua protezione rappresentano adeguata ricompensa per le eventuali attività straordinarie svolte ai fini del soccorso, pertanto non è dovuto compenso alcuno per i servizi resi nell'ambito del presente accordo.".
Se i firmatari dell'accordo decidono invece di prevedere un compenso forfetario per le attività di soccorso, è necessario specificarlo in questa clausola:
"a titolo di parziale ristoro degli oneri sostenuti dell'organizzazione soccorritrice per l'espletamento delle attività di propria competenza previste nel presente accordo e nel piano di continuità operativa, l'organizzazione in emergenza che venga ospitata dall'organizzazione soccorritrice verserà a quest'ultima un contributo forfetario ed omnicomprensivo di € …… (……) con le modalità di seguito riportate …".

Periodo di validità dell'accordo
E' opportuno venga sempre indicato un periodo di validità dell'accordo (3-7 anni). Scaduto il termine, le parti potranno rinnovare l'accordo modificandone eventualmente le condizioni.

Recesso
Va indicata la possibilità di recesso dall'accordo. Di regola ciascuna parte può recedere dall'accordo in qualunque momento, senza necessità di motivare tale decisione, dandone comunicazione scritta alle altre parti. Può essere previsto un periodo di preavviso prima del recesso.

Responsabilità delle parti in caso di recesso
Questa clausola riporta le responsabilità delle parti in caso di recesso dall'accordo oppure per il mancato o parziale intervento a seguito di una formale richiesta di soccorso.
Di norma i patti di mutuo soccorso non prevedono alcuna responsabilità [12]:
nessuna delle parti firmatarie è responsabile nei confronti delle altre parti per gli effetti derivanti dal recesso dal presente accordo; le parti non sono altresì responsabili per le conseguenze dovute a carenza o difformità di assistenza rispetto a quanto previsto nel presente accordo.

CLAUSOLE CHE REGOLAMENTANO LE ATTIVITÀ DI MUTUO SOCCORSO

Prove periodiche
Nel caso si prevedano prove periodiche congiunte, è opportuno venga sempre indicato un periodo di validità dell'accordo (3-7 anni):
le parti concordano di eseguire prove congiunte dei rispettivi piani di continuità operativa al fine di verificarne l'efficacia. Le prove si svolgeranno almeno con cadenza annuale simulando a turno la condizione di crisi per ciascuna organizzazione aderente al presente accordo.

Modalità di richiesta del soccorso
Deve essere esplicitato il modo in cui sarà richiesta l'attivazione del processo di soccorso. In particolare è opportuno stabilire:
- i soggetti autorizzati ad inoltrare la richiesta di soccorso (vertice dell'organizzazione, responsabile della sicurezza, soggetto terzo, ecc.);
- la procedura con cui sarà inoltrata la richiesta (ad esempio tramite chiamata telefonica confermata entro 24 ore da una richiesta scritta);
- le informazioni che devono accompagnare la richiesta di soccorso (motivazione della richiesta, tipologia di servizi necessari, punti di contatto, ecc.).

[12] Si vuole osservare che, benché l'assenza di responsabilità possa fare apparire l'accordo particolarmente "debole", all'atto pratico la naturale solidarietà che si manifesta in occasione di eventi calamitosi rende il patto efficace. Ciò nondimeno è possibile prevedere alcune responsabilità per rendere l'accordo maggiormente vincolante.

Organizzazione soccorritrice

Nel caso l'accordo riguardi più di due organizzazioni, è opportuno chiarire la logica con cui sarà individuata l'organizzazione soccorritrice. Le possibilità sono:

- scelta autonoma dell'organizzazione in emergenza;
- scelta secondo una logica predeterminata (ad esempio secondo una scala di priorità basata sulle distanze geografiche tra i siti);
- scelta effettuata da un ente terzo che svolge il ruolo di coordinatore dei soccorsi.

E' anche opportuno chiarire se la stessa richiesta di soccorso può essere inoltrata contemporaneamente a più enti.

Compiti del destinatario di una richiesta di soccorso

Vanno descritti gli impegni assunti dall'organizzazione che riceve una richiesta di soccorso.

Ad esempio:

"l'organizzazione che riceve richiesta di assistenza intraprenderà, secondo il piano temporale concordato con la parte richiedente, le azioni necessarie per ripristinare i servizi informatici essenziali ed a tal fine renderà disponibili i locali, gli arredi, gli apparati, i materiali e le altre risorse occorrenti per erogare il servizio in condizioni di emergenza [13]*.* ".

Condizioni di deroga agli obblighi di soccorso

Vanno elencate le eventuali condizioni che sollevano l'organizzazione che riceve una richiesta di soccorso dagli obblighi di cui al punto precedente.

Ad esempio:

"l'organizzazione che riceve richiesta di assistenza non è tenuta a svolgere le attività richieste se:

- *è anch'essa in uno stato di emergenza, per un evento calamitoso o altre cause impreviste;*
- *ha già avviato una procedura di soccorso a favore di un ente che partecipa all'accordo*.".

Comitato di crisi

Può essere opportuno prevedere la costituzione di un comitato di crisi che comprenderà sia esperti dell'organizzazione in stato di emergenza che dell'organizzazione soccorritrice. Il comitato di crisi può essere costituito anticipatamente (soluzione consigliabile) o al momento in cui si verifica la condizione di emergenza. Tra i compiti tipici del comitato di crisi:

- la validazione dei piani di continuità operativa;
- la pianificazione ed il controllo delle eventuali prove;
- il coordinamento delle attività relative al recupero dei dati, il ripristino dei servizi, l'esercizio in condizioni di emergenza ed il rientro alla normalità.
-

Coordinamento delle attività

E' opportuno precisare la responsabilità del coordinamento delle attività che saranno svolte durante le prove ed in condizioni di emergenza. L'approccio tipico consiste nel definire una struttura di coordinamento cui partecipano sia l'ente in emergenza che quello ospitante. Tale struttura può coincidere con il comitato di crisi.

Ad esempio:

"le attività relative al ripristino dei servizi informatici, la loro erogazione in condizioni di emergenza ed il rientro alle condizioni ordinarie, saranno coordinate dal comitato di crisi di cui al punto …. Il personale della parte soccorritrice incaricato delle attività di assistenza, pur conservando l'organizzazione ed i riporti correnti, opererà coerentemente con le indicazioni fornite dal comitato di crisi.".

[13] L'elenco delle risorse che saranno rese disponibili in condizioni di emergenza può essere contenuto in un documento, concordato tra le parti, redatto in occasione della definizione del piano d'emergenza ed aggiornato periodicamente: in questo caso la clausola relativa agli obblighi può fare esplicito riferimento a tale documento.

Durata massima dell'attività di soccorso

Si tratta di una clausola molto importante perché salvaguarda l'Amministrazione soccorritrice da una permanenza eccessiva dell'ente in emergenza presso il proprio sito.

In genere viene indicato un termine massimo, trascorso il quale l'organizzazione in emergenza è tenuta ad abbandonare il sito ospitante.

Una soluzione alternativa consiste nel prevedere che le due organizzazioni (o il comitato di crisi) sviluppino concordemente un piano di rientro che terrà conto delle specificità del disastro: in tale caso l'organizzazione in emergenza si impegna a rispettare i tempi di tale piano.

CLAUSOLE DI TUTELA

Riservatezza delle informazioni

E' opportuno che le parti si impegnino a non divulgare le informazioni di cui verranno a conoscenza nell'espletamento delle attività di mutuo soccorso:

"le parti sono tenute ad assicurare la riservatezza delle informazioni, dei documenti e degli atti amministrativi dei quali vengano a conoscenza durante l'esecuzione del presente accordo ed inoltre si impegnano a rispettare rigorosamente tutte le norme relative alla tutela della riservatezza dei dati personali.".

Limiti di applicabilità dell'accordo

Può essere utile introdurre una clausola che tuteli nei confronti di un uso "improprio" dell'accordo, ad esempio per utilizzare senza compensi la consulenza di esperti di un'altra organizzazione.

Ad esempio:

"il presente accordo non può essere utilizzato in alcun modo per giustificare attività o accordi tra le organizzazioni, o tra il personale delle medesime, che siano al di fuori del mero obiettivo di reciproco soccorso a seguito di eventi imprevisti e calamitosi.".

Responsabilità nei confronti di terzi

Occorrerebbe definire le responsabilità delle parti relativamente ad eventuali danni che possono essere arrecati a terzi nel periodo in cui l'organizzazione soccorritrice ospita l'organizzazione in emergenza.

In generale è tutelata l'organizzazione ospitante che non è responsabile per i danni arrecati in conseguenza dei servizi erogati in condizioni di emergenza, a meno che essi non siano dovuti a comportamenti negligenti o malevoli del proprio personale.

Interpretazione dell'accordo

Può essere utile prevedere una modalità operativa per risolvere controversie derivanti da una diversa interpretazione dell'accordo.

Ad esempio:

"qualora dovessero insorgere difformità interpretative tra le parti in ordine alle disposizioni e clausole contenute nel presente accordo, le parti medesime concordano che provvederanno alla bonaria risoluzione delle difformità di cui sopra mediante appositi incontri che saranno fissati allo scopo di raggiungere un'interpretazione comune; qualora non dovesse essere raggiunta una posizione comune tra le parti, le medesime rimetteranno la decisione ad un Collegio arbitrale composto da tre membri di cui due nominati dalle parti in contenzioso, ed il terzo di comune accordo dagli arbitri nominati dalle parti.".

APPENDICE E: ESEMPI DI LDS

E’ opportuno siano definiti appositi livelli di servizio e penali per i vari adempimenti richiesti dal fornitore tenuto conto dei manuali e lemmi delle linee guida sulla qualità dei beni e servizi ICT, regolamentando, al di là dei Tier individuati, i termini e le modalità degli adempimenti richiesti nonché i valori di RPO e RTO ed eventualmente avvalendosi (contestualizzandole alla tipologia di contratto/servizio richiesto) di quelli di seguito esemplificati:

Adempimento prescritto	**Inadempimento; casi in cui si applica la penale**	**Soglia/ metrica**	**Aspetti e dati elementari da verificare. Eventuale formula di calcolo. Finestra temporale**	**Penale applicabile in caso di inadempimento e/o scostamento dalle soglie prescritte (**da applicare per tutto il tempo dell’inadempienza, dal giorno di contestazione e fino al giorno nel quale sarà risolta l’inadempienza)	**Ambito di applicabilità dell’adempimento/ indicatore; soluzione e casi cui si può adattare**
Dare avvio al servizio richiesto tempestivamente e correttamente.	Mancato/tardato avvio del contratto o dei servizi/attività rispetto ai termini previsti	Giorno solare	Verificare che le attività e servizi richiesti risultino avviati e completati nei tempi e correttamente. Verificare sia il mancato avvio del servizio in generale dal mancato avvio/ completamento delle attività comprese nel servizio ad es. graduando la penalità in considerazione dell’importan-za dell’attività non svolta, avviata/completata tardivamente.	In caso di ritardo nell’avvio e completamento delle attività e servizi richiesti sarà applicata una penale pari al XX% del corrispettivo mensile complessivo previsto sia per ciascuno giorno solare di ritardo (nell’avvio/nel completamento) sia per ciascun inadempimento	Ambito di applicabilità abbastanza generale; assicura la tempestività di avvio e completamento delle attività e servizi; si può adattare a qualsiasi soluzione tecnica di DR scelta.

Adempimento prescritto	**Inadempimento; casi in cui si applica la penale**	**Soglia/ metrica**	**Aspetti e dati elementari da verificare. Eventuale formula di calcolo. Finestra temporale**	**Penale applicabile in caso di inadempimento e/o scostamento dalle soglie prescritte** (da applicare per tutto il tempo dell'inadempienza, dal giorno di contestazione e fino al giorno nel quale sarà risolta l'inadempienza)	**Ambito di applicabilità dell'adempimento/ indicatore; soluzione e casi cui si può adattare**
Rispetto del livello di servizio relativo all'RTO	Mancata attivazione della Configurazione di Emergenza/ Simulazione entro l'RTO previsto	La metrica dipende da quanto previsto per l'RTO (a seconda che si sia definito in termini di ore, giorni, settimane ecc.)	RTO = RTO atteso – RTO effettivamente assicurato (da applicare e verificarne l'osservanza sia durante i test/le simulazioni/test o in caso di emergenza)	Per ciascuno scostamento dai valori di RTO e per ciascun caso di indisponibilità e ritardo nell'attivazione della configurazione di emergenza, sarà applicata una penale pari: - all' XXX% del corrispettivo complessivo mensile previsto se il ritardo è riscontrato in occasione dello svolgimento dei test/delle simulazioni; - all' XXX% del canone complessivo mensile previsto se il ritardo è riscontrato durante la permanenza presso il Sito di DR in condizioni di emergenza	Ambito di applicabilità generale; è un indicatore essenziale alla verifica del corretto svolgimento del servizio di DR. Va definito tenuto conto del contesto tecnico operativo, della BIA, dello SFT e della soluzione adottata

Adempimento prescritto	**Inadempimento; casi in cui si applica la penale**	**Soglia/ metrica**	**Aspetti e dati elementari da verificare. Eventuale formula di calcolo. Finestra temporale**	**Penale applicabile in caso di inadempimento e/o scostamento dalle soglie prescritte (**da applicare per tutto il tempo dell'inadempienza, dal giorno di contestazione e fino al giorno nel quale sarà risolta l'inadempienza)	**Ambito di applicabilità dell'adempimento/ indicatore; soluzione e casi cui si può adattare**
Rispetto del valore di RPO (perdita dati tollerabile in termini di scostamento fra l'immagine dei dati del sito secondario rispetto ai dati del sito primario) da verificare entro un finestra temporale definita (es. con cadenza giornaliera; settimanale; mensile). Va rispettato e verificato periodicamente, in occasione dei test/simulazioni di disaster e in caso di attivazione della configurazione di emergenza.	Perdita dati superiore ai valori e inconsistenza dei dati di copia/backup	% Es. un RPO tale che il 99% dei dati copiato nella finestra temporale prevista sia correttamente effettuato e sia allineato ai dati del sistema primario	Nella finestra temporale prevista per il monitoraggio dell'indicatore verranno effettuati dei campionamenti ad intervalli di tempo predefiniti. Es. se la finestra è giornaliera Chiamati "*N fuori soglia*" i campioni con RPO > RPOs e "*NT=numero campiona-menti giornalieri*", e tenuto conto di *N= numero giorni della settimana* il livello di servizio da garantire sarà calcolato con la formula seguente: Δ percentuale = (NT – N fuori soglia)/ NT *100 >/= 99 %	Per ogni punto percentuale di scostamento dalla soglia definita, nonché per ogni caso di verificata inconsistenza dei dati di replica verrà applicata una penale pari allo 0,1% del corrispettivo mensile complessivo previsto	Ambito di applicabilità generale; è un indicatore essenziale alla verifica del corretto svolgimento del servizio di DR. Va definito tenuto conto del contesto tecnico operativo, della BIA, dello SFT e della soluzione adottata Va rispettato e verificato in occasione dei test/ simulazioni di disaster e in caso di attivazione della configurazione di emergenza.
Garantire la tempestività di ripristino in caso di guasto, malfunzionamento o anomalie di tutte le componenti, anche ridondate, del servizio di DR, assicurandone la manutenzione e la perfetta efficienza. Garantire il mantenimento delle risorse messe a disposizione in condizioni di normale operatività con obbligo di ripristinare la funzionalità tempestivamente.	Ritardo nel ripristino della funzionalità a fronte di guasti, malfunzionamenti o anomalie delle componenti, anche ridondate, necessarie al servizio di DR	Ore/giorni di indisponibilità e ritardo nel ripristino, rispetto ai termini di ripristino definiti a decorrere dal momento della segnalazion pervenuta.	DOS – DORipr. = 0 Ove: -DOS = Data e ora di segnalazione del guasto, malfunzionamento/anomalia -DORipr. = Data e ora di chiusura dell'intervento col ripristino della funzionalità. I termini di ripristino saranno calcolati a a decorrere dal momento della segnalazione comunque pervenuta	Per ciascuna ora di indisponibilità o per ciascuna ora di ritardo nel ripristino della funzionalità di tutte le componenti, anche ridondate, necessarie al servizio di DR, sarà applicata una penale pari, rispettivamente, allo XX% del corrispettivo complessivo mensile previsto, per le inadempienze riscontrate in condizioni normali e una penale pari all'XX% del corrispettivo complessivo mensile previsto, nel caso di inadempienze riscon-trate in situazione di emergenza	Ambito di applicabilità generale. E' opportuno definire i termini e le modalità di segnalazione/apertura dell'intervento per il ripristino del malfunzionamento; si possono graduare le penalità anche a seconda dell'importanza che il componente riveste nell'ambito della soluzione di DR. Per essere effettivamente applicabile richiede strumenti di verifica, rendicontazione ed eventualmente monitoraggio da remoto.

Adempimento prescritto	**Inadempimento; casi in cui si applica la penale**	**Soglia/ metrica**	**Aspetti e dati elementari da verificare. Eventuale formula di calcolo. Finestra temporale**	**Penale applicabile in caso di inadempimento e/o scostamento dalle soglie prescritte** (da applicare per tutto il tempo dell'inadempienza, dal giorno di contestazione e fino al giorno nel quale sarà risolta l'inadempienza)	**Ambito di applicabilità dell'adempimento/ indicatore; soluzione e casi cui si può adattare**
Garantire la disponibilità delle risorse e componenti necessarie alla soluzione di DR previste	Indisponibilità del numero e tipologia delle risorse previste e necessarie all'erogazione dei servizi di DR che possano avere impatto sulla soluzione di DR richiesta	% / nr. di risorse effettivamente disponibili (per numero e tipologia) es. nella finestra temporale mensile	Risorse Previste nel mese di riferimento – Risorse Disponibili nel mese di riferimento / Risorse Previste nel mese di riferimento	Per ciascun caso di inadempimento (numero in meno o punto percentuale in meno rispetto alla soglia prevista/al numero e tipologia di risorse, verrà applicata una penale pari, rispettivamente, allo XX% del corrispettivo complessivo mensile previsto, per le inadempienze riscontrate in condizioni normali e una penale pari all'XX% del corrispettivo complessivo mensile previsto, nel caso di inadempienze riscontrate in situazione di emergenza	Da prevedere quando si sia espressamente richiesta la disponibilità di un certo tipo e numero di risorse/componenti (es. server, risorse elaborative; TB ; storage; connettività ecc.ecc.). Può essere opportuno anche graduare la penalità da applicare tenuto conto della rilevanza e dell'importanza che la risorsa riveste nell'ambito della soluzione di DR. Per essere effettivamente applicabile richiede strumenti di verifica, rendicontazione e eventualmente monitoraggio da remoto.
Garantire la disponibilità degli spazi richiesti (in termini di MQ e caratteristiche e requisiti)	Indisponibilità/inadeguatezza rispetto alle caratteristiche e requisiti del numero e tipologia degli spazi richiesti e necessari all'erogazione dei servizi di DR	Per ciascun caso di inadempimento (numero di mq in meno o inadeguatezza rispetto alle caratteristiche e requisiti degli spazi) verrà applicata una penale pari, rispettivamente, allo XX% del corrispettivo complessivo mensile previsto, per le inadempienze riscontrate in condizioni normali e una penale pari all'XX% del corrispettivo complessivo mensile previsto, nel caso di inadempienze riscontrate in situazione di emergenza			Da prevedere se si sia espressamente richiesta la dispo-nibilità di un certo tipo e numero di spazi (housing). Può essere anche un aspetto attinen-te alla fase di collaudo e test e ricadere negli adempimenti affidati al fornitore per il superamento del collaudo/o del test
Assicurare il tempestivo e corretto svolgimento dei test periodici. I test periodici dovranno essere svolti nel rispetto dei termini previsti, in modo adeguato/rispondente a quanto prescritto dal piano di continuità /DR	In caso di ritardata esecuzione dei test periodici	Giorno solare di ritardo	Riscontro del ritardo/mancata esecuzione del test per cause imputabili al fornitore.	Per ogni giorno solare di ritardo nell'esecuzione dei test, sarà applicata una penale pari allo XXX % del corrispettivo comples-sivo mensile previsto	Ambito di applicabilità generale; è un indicatore essenziale alla verifica del corretto svolgimento del servizio di DR.

Adempimento prescritto	**Inadempimento; casi in cui si applica la penale**	**Soglia/ metrica**	**Aspetti e dati elementari da verificare. Eventuale formula di calcolo. Finestra temporale**	**Penale applicabile in caso di inadempimento e/o scostamento dalle soglie prescritte** (da applicare per tutto il tempo dell'inadempienza, dal giorno di contestazione e fino al giorno nel quale sarà risolta l'inadempienza)	**Ambito di applicabilità dell'adempimento/ indicatore; soluzione e casi cui si può adattare**
Svolgere e concludere con esito positivo i test periodici.	Esito del test negativo imputabile al fornitore.	n.a.	In caso di esito negativo del test, il fornitore dovrà richiedere la convocazione di una nuova seduta con apposita richiesta di ripetizione del test (ove attesti che ha risolto le situazioni che non hanno reso possibile concluderlo con esito favorevole).	Nel caso in cui l'esecuzione del test si concluda con esito negativo si applicherà una penale pari allo xx % del corrispettivo complessivo mensile previsto per ogni giorno intercorrente tra quello successivo alla data di svolgimento del test e quello immediatamente precedente alla data di svolgimento del 2° test. Es. Nel caso in cui anche l'esecuzione del 2° test si concluda nuovamente con esito negativo, sarà applicata una penale pari al doppio della penale applicata a seguito dell'esito negativo del test a partire dalla data della prima seduta di test conclusasi con esito negativo	Ambito di applicabilità generale; è un indicatore essenziale alla verifica del corretto svolgimento del servizio di DR.
Predisporre e consegnare entro i termini previsti i deliverable richiesti	Ritardo nella consegna dei deliverable. Ai fini dell'adempimento si intendono oggetto di verifica sia i termini previsti per la consegna che i termini previsti per la consegna a seguito di eventuali richieste di modifiche/ integrazioni/correzioni	Giorno solare	Ritardo nel rispetto dei termini previsti. Data prevista di consegna – data di effettiva consegna del deliverable Verifica che siano rispettati i termini di consegna dei deliverable	Per ogni giorno solare di ritardo, per ogni inadempienza riscontrata e per ogni deliverable non consegnato nei termini previsti si potrà applicare una penale pari allo XXX % del corrispettivo complessivo mensile previsto.	Ambito di applicabilità abbastanza generale; assicura la tempestività di consegna dei deliverable; si può adattare a qualsiasi soluzione tecnica di DR scelta

Adempimento prescritto	**Inadempimento; casi in cui si applica la penale**	**Soglia/ metrica**	**Aspetti e dati elementari da verificare. Eventuale formula di calcolo. Finestra temporale**	**Penale applicabile in caso di inadempimento e/o scostamento dalle soglie prescritte** (da applicare per tutto il tempo dell'inadempienza, dal giorno di contestazione e fino al giorno nel quale sarà risolta l'inadempienza)	**Ambito di applicabilità dell'adempimento/ indicatore; soluzione e casi cui si può adattare**
Svolgere in modo tempestivo e corretto i collaudi/le verifiche di conformità ove previste, con superamento, delle stesse con esito favorevole. Le attività suscettibili di collaudo/verifica di conformità dovranno essere completate secondo quanto previsto nel piano di collaudo, con la comunicazione di "pronti al collaudo e alla verifica e la consegna dei deliverable previsti. L'esito delle attività svolte/dei servizi dovrà essere sottoposto a 1° collaudo/ verifica di conformità entro i termini previsti. La 2° seduta di collaudo/verifica di conformità dovrà essere svolta entro i termini previsti a decorrere dalla data della 1° seduta di collaudo/ verifica di conformità conclusesi con esito negativo	Esito negativo del collaudo. In caso di esito negativo del 1° collaudo/della 1° verifica di conformità il fornitore dovrà richiedere la convocazione di una nuova seduta di collaudo/verifica di conformità con apposita richiesta di ripetizione del collaudo/della verifica di conformità, ove attesti che ha risolto le situazioni che non hanno reso possibile superare, con esito favorevole, il primo/la prima verifica di conformità.	Giorno solare di ritardo	Esito negativo del collaudo/ della verifica di conformità o tradiva convocazione del collaudo/della verifica di conformità per cause imputabili al fornitore.	Per ciascun giorno successivo alla data del verbale da cui risulti l'esito negativo del collaudo/della verifica di conformità sarà applicata una penale pari allo xx % del corrispettivo complessivo mensile contrattuale dal 1° al 10° giorno e una penale pari allo xx % del corrispettivo complessivo mensile previsto dall'11° al 30° giorno. Nel caso in cui anche il secondo collaudo/ la seconda verifica di conformità si concluda con esito negativo sarà applicata una penale in misura doppia rispetto a quella prevista per il tardivo e negativo esito del collaudo/della verifica di conformità, per tutti i giorni che intercorrono fra la data del verbale del primo collaudo/della prima verifica di conformità con esito negativo e la data del verbale del secondo collaudo/della seconda verifica di conformità, con esito negativo.	Ambito di applicabilità generale; è un indicatore essenziale alla verifica della soluzione di DR realizzata ma anche, in corso di contratto/erogazione dei servizi ove si renda necessario effettuare delle verifiche di conformità sul corretto svolgimento del servizio di DR.

Adempimento prescritto	**Inadempimento; casi in cui si applica la penale**	**Soglia/ metrica**	**Aspetti e dati elementari da verificare. Eventuale formula di calcolo. Finestra temporale**	**Penale applicabile in caso di inadempimento e/o scostamento dalle soglie prescritte (**da applicare per tutto il tempo dell'inadempienza, dal giorno di contestazione e fino al giorno nel quale sarà risolta l'inadempienza)	**Ambito di applicabilità dell'adempimento/ indicatore; soluzione e casi cui si può adattare**
Garantire - sia in caso di sostituzione o aggiorna-mento tecnologico degli apparati di storage collocati presso il sito di DR o di parte di essi, sia al termine del contratto, su richiesta dell'Amministrazione la cancellazione dei dati contenuti negli apparti usati per la soluzione di CO/DR. Garantire la cancella-zione delle copy utilizzate per il test al termine dello stesso.	Qualora si riscontri la mancata cancellazione dei dati o l'inadeguatezza o l'incompletezza delle attività connesse alla cancellazione certificata dei dati, nonché la cancellazione delle e flash copy utilizzate per il test al termine dello stesso.	Per ciascun caso di riscontrata inadempienz a e per ciascun giorno di contestata inadempienz a	Verifica che la cancellazione delle copy utilizzate per il test, al termine dello stesso e che la cancellazione dei dati dallo storage o da parti di esso risulti effettuata in modo non adeguato o incompleto – sia nel corso del contratto, in caso di sostituzione o aggiornamento tecnologico in modo adeguato e/o completo sia al termine del contratto – sarà applicata la penale conteggiando tutti i giorni per cui perduri la situazione di non conformità contestata	Per ciascun giorno di contestata inadempienza, sarà applicata una penale pari: all'xxx% del corrispettivo complessivo mensile previsto	Ambito di applicabilità generale. Utile quando si voglia avere certezza dell'avvenuta cancellazione di dati particolarmente critici da apparati non di proprietà dell'Amm.ne che fruisce del servizio di DR. Rende opportuno definire come verificare l'avvenuta cancellazione
Assicurare che le risorse professionali messe a disposizione per l'erogazione dei servizi, abbiano le competenze, il mix e ed esperienze richieste, risultino inviati i curricula, siano sostituite se non gradite o nei casi previsti entro i termini definiti non siano sostituite per più di due volte nel periodo di vigenza del contratto, siano sostituite con risorse con competen-ze ed esperienze equi-pollenti o superiori a quelle da sostituire.	Per i casi di mancato rispetto degli obblighi definiti per quel che attiene alle risorse professionali messe a disposizione per l'erogazione dei servizi ovvero per i casi in cui: - non venga rispettato il mix minimo previsto e dettagliato nel Piano di progetto; -non vengano forniti i curricula delle risorse professionali o detti curricula non consentano di avere chiare le competenze ed esperienze delle risorse professionali messe a disposizione per l'erogazione dei servizi; - non venga sostituita la risorsa per la quale è stato espresso il mancato gradimento; - venga superato il numero massimo di sostituzioni consentite nell'arco di vigenza del contratto; - non venga proposta in sostituzione una risorsa in possesso di competenze ed esperienze equipollenti o superiori a quella da sostituire, - verrà applicata una penale pari all'XXX% del corrispettivo complessivo mensile previsto a partire dalla data della comunicazione di contestazione dell'inadempienza.				Può esser neces-sario solo laddove il requisito delle risorse professio-nali per l'erogazio-ne dei servizi di DR abbia una rilevanza parti-colare per l'Amministrazione che fruisce della soluzione di DR. Rende opportuno definire il mix che si richiede e prevedere strumenti di verifica e controllo delle risorse messe a disposizione.