e atteso entro il 2011, è quello che assorbirà lo standard BS 25999-2 in uno standard internazionale, dando così notevole ulteriore impulso alla certificazione della CO.

3.6.1 Gli standard ISO 22399 e ISO 223011

Riprendendo lo schema familiare di alcuni standard del BSI, anche 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 22399**, emesso nel 2007, descrive le buone pratiche in materia di CO. Si tratta, anzi, di un ISO/PAS (cioè un "publicly available specification", che rende questa norma ancora più tenue in termini di osservanza e ne fa una mera indicazione di opportunità), che ha il titolo di "Societal security — Guideline for incident preparedness and operational continuity management";
- lo standard **ISO 22301** ("Societal security -- Preparedness and continuity management systems – Requirements"), che sarà emesso nel corso del 2011, tratta invece del sistema di gestione della CO e delle verifiche, che implica un percorso di certificazione.

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 del BS 25999 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. Lo standard ISO 27031 dovrebbe aiutare a rendere più determinato questo percorso.

[1] Nel caso dello standard ISO 22301, che si trova ancora nello stato di DIS (draft international standard), la numerazione potrebbe differire nella versione finale.

3.6.2 Lo standard ISO 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 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 e, pertanto, lo standard costituisce un ottimo punto di riferimento per la costruzione di gare destinate alla ricerca di un servizio di Disaster Recovery.

3.6.3 Lo standard ISO 27031

Nel marzo 2011 è stato pubblicato lo standard **ISO 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 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.

3.6.4 Lo standard della sicurezza ISO 27002

Questo standard ("Information technology -- Security techniques -- Code of practice for information security management"), piuttosto noto, rappresenta, con lo standard ISO 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.

3.7 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.

3.7.1 ITIL

L'ITIL ("Information Technology Infrastructure Library") 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

3.8 NFPA 1600

NFPA ("National Fire Protection Association") è l'associazione per la protezione contro gli incendi degli Stati Uniti, creata nel 1896. Dal gennaio 2000 NFPA pubblica uno standard, **NFPA 1600** ("Standard on Disaster/Emergency Management and Business Continuity Programs"), che propone un insieme di criteri per la gestione delle catastrofi. Lo standard (del tipo "buone pratiche"), giunto nel 2010 alla terza revisione, fornisce indicazioni per la politica della continuità, i comitati di gestione delle emergenze, la classificazione di rischi e minacce. Questo standard ha avuto qualche influenza nella predisposizione dello standard ISO 22301.

4 ORGANIZZAZIONE DELLE STRUTTURE DI GESTIONE DELLA CONTINUITÀ OPERATIVA E INDICAZIONI UTILI ALL'ATTUAZIONE DELLE SOLUZIONI DI SALVAGUARDIA DEI DATI E DELLE APPLICAZIONI

Questo capitolo propone consigli e indicazioni su come creare e organizzare, all'interno di una Pubblica Amministrazione, le strutture incaricate di gestire le problematiche della continuità operativa.

La struttura organizzativa preposta a gestire le problematiche di continuità operativa all'interno di un'amministrazione ha per definizione la missione di:

- predisporre tutte le misure necessarie per ridurre l'impatto di un'emergenza;
- mettere a disposizione risorse alternative a quelle non disponibili;
- governare il sistema durante l'emergenza;
- gestire il rientro alla normalità.

In condizioni ordinarie, la suddetta struttura pianifica e definisce le attività necessarie ad affrontare le emergenze, adotta opportuni strumenti e adeguate soluzioni tecnologiche, fa in modo che i suoi componenti abbiano un'elevata sensibilità nei confronti delle attività e delle capacità richieste affinché il processo di mantenimento della continuità operativa abbia successo.
In condizioni di emergenza la struttura assicura l'ordinato svolgimento di una molteplicità di azioni, a partire dalla gestione delle operazioni tecniche alle comunicazioni.
In condizioni di emergenza risulta di fondamentale importanza saper identificare il carattere critico di un evento che impatta sull'organizzazione, anche ricorrendo all'adozione di un sistema di metriche di riferimento calibrate sull'esperienza quotidiana.
Non tutti gli eventi critici evolvono in un disastro; non è quindi sempre necessario attivare i processi definiti per il ripristino: ciò dipende dall'impatto dell'evento che si è verificato sui servizi critici dell'amministrazione.

È opportuno, perciò, che chi opera e vigila sulla corretta erogazione dei servizi critici disponga di criteri oggettivi sulla base dei quali:

- valutare la portata dell'evento e la sua effettiva gravità;
- scegliere se innescare o no i processi definiti per il ripristino.

A titolo di esempio, vengono di seguito elencate alcune condizioni (in termini di conseguenza di un evento) che determinano senz'altro la necessità di attivare i processi di ripristino:

- distruzione delle infrastrutture del CED dell'amministrazione;
- impossibilità di accedere ai locali del CED o di controllare il funzionamento degli apparati in esso ospitati per un tempo indeterminato;
- impossibilità di erogare servizi a un'utenza considerevole o significativa;
- impossibilità di controllare l'esercizio delle applicazioni, con grande indeterminatezza sia per l'estensione del danno che per la sua durata.

Come ulteriore indicazione, è fortemente consigliabile predisporre e aggiornare l'elenco dei servizi e delle applicazioni critiche (vedi capitolo 5 ed appendice A). Nel citato elenco saranno specificate, per ogni elemento dell'elenco, le condizioni di attenzione, superate le quali si deve attivare la struttura dedicata alla continuità. Le condizioni di attenzione possono ad esempio essere espresse in termini di:

- numero massimo di segnalazioni di malfunzionamento eseguite dagli utenti del servizio in un dato intervallo temporale;
- intervallo di tempo massimo in cui il sistema risulta inoperoso (oltre tale durata, probabilmente c'è un problema sulla rete o altrove che impedisce agli utenti di accedere al sistema).

A seconda dell'impatto del singolo evento ed in relazione alle caratteristiche dell'organizzazione, l'ente potrà determinare il livello di gravità a partire dal quale sarà necessario attivare le procedure di continuità previste dal Piano.

4.1 Coinvolgimento dei vertici dell'amministrazione e ruolo della struttura di gestione

Per garantire l'efficacia della soluzione di continuità, in genere è necessario che:

- la struttura organizzativa definita e in generale l'intera soluzione siano condivisi, promossi e sostenuti, con un chiaro mandato, dai massimi vertici dell'amministrazione, previa condivisione con il Responsabile della sicurezza (vgs. artt. 51 e 71 del CAD);
- quanto progettato venga promulgato attraverso atti e documenti specifici;
- sia nominato il "Responsabile della continuità operativa" dell'ente;
- vengano istituite ufficialmente le relative strutture organizzative, allocando le necessarie risorse umane ed economiche ed attribuendo gli opportuni livelli di responsabilità interna ed esterna;
- siano definite le figure di "*alternate*" dei vari incaricati della gestione della CO ed una precisa escalation gerarchica per le decisioni.

È, infatti, opportuno che la struttura organizzativa definita per la continuità abbia responsabilità e compiti ben definiti, e che possieda ampia autonomia decisionale e disponibilità di utilizzare risorse straordinarie.
È senz'altro preferibile che il governo dell'emergenza sia affidato a un unico centro di responsabilità - articolato diversamente ed in ragione delle caratteristiche dimensionali, organizzative e geografiche dell'ente - che sia abilitato a riportare direttamente ai vertici dell'organizzazione.
L'identificazione delle figure cui sarà demandato il compito di formare il "Comitato di gestione della crisi" non può comunque prescindere dalle attribuzioni previste in capo all'Unità Locale per la Sicurezza (ULS), la componente istituita all'interno di ogni amministrazione per il governo degli aspetti di sicurezza relativi all'adesione al Sistema Pubblico di Connettività.
Ai sensi dell'art. 21, co.9 del DPCM 01.04.2008 (Regole Tecniche e di sicurezza per il funzionamento dell'SPC), l'Unità locale di sicurezza svolge i seguenti compiti (anche avvalendosi dei fornitori qualificati):

a) garantire, anche per il tramite di un fornitore qualificato, la realizzazione ed il mantenimento dei livelli di sicurezza previsti per il dominio di competenza;
b) garantire che la politica di sicurezza presso la propria organizzazione sia conforme agli indirizzi e alle politiche di sicurezza definite dalla Commissione;

c) interagire con la struttura centrale per raccogliere, aggregare e predisporre nel formato richiesto le informazioni necessarie per verificare il livello di sicurezza dell'SPC;
d) notificare alla struttura centrale ed al CERT-SPC, secondo le modalità stabilite, eventuali incidenti informatici o situazioni di criticità o vulnerabilità delle infrastrutture SPC locali;
e) adottare le necessarie misure volte a limitare il rischio di attacchi informatici ed eliminare eventuali vulnerabilità della rete, causate dalla violazione e utilizzo illecito di sistemi o infrastrutture della Pubblica Amministrazione.

L'organizzazione ed il dimensionamento delle ULS sono fortemente condizionate dalla caratteristiche dell'ente ma, nella maggior parte dei casi, si tratta di strutture (o meglio funzioni) distribuite all'interno dell'ente medesimo e differenziate per capacità e responsabilità di intervento su contesti o per tecnologie di riferimento.
Procedendo per analogia sarà possibile identificare dei responsabili di riferimento per ciascuno dei servizi identificati come critici a seguito dell'analisi di impatto (BIA) ed adottare i medesimi canali di comunicazione previsti per i referenti ed il responsabile della ULS; questi, coordinati dalla designanda figura del responsabile per la continuità operativa dell'amministrazione, rappresenteranno *de facto* i componenti del comitato di gestione della crisi.

4.2 Il Comitato di gestione della crisi

Il Comitato di gestione della crisi è, pertanto, 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 della crisi e, inoltre, ha la responsabilità di garanzia e controllo sull'intero progetto.
Le figure minime necessarie per la costituzione del Comitato di gestione della crisi sono rappresentate da:

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

I principali compiti del Comitato sono:

- definizione ed approvazione del piano di continuità operativa;
- valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi;
- avvio delle attività di recupero e controllo del loro svolgimento;
- rapporti con l'esterno e comunicazioni ai dipendenti;
- attivazione del processo di rientro che deve essere attuato da specifici gruppi operativi, ma deve essere continuamente monitorato dal Comitato, per assicurare la verifica dello stato di avanzamento complessivo e risolvere i casi dubbi. Infatti, per loro natura le operazioni di rientro, per quanto dettagliate, possono presentare imprevisti o azioni che coinvolgono altre persone e hanno impatto su molteplici attività. In tutti questi casi il Comitato deve acquisire tutti gli elementi utili a condurre alla soluzione del problema;
- avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
- dichiarazione di rientro;

- gestione di tutte le situazioni non contemplate;
- gestione dei rapporti interni e risoluzione dei conflitti di competenza (la gestione dei rapporti interni è di primaria importanza: in situazione d'emergenza, caratterizzata da incertezze, difficoltà di comunicazione, stress, nervosismo e stanchezza, il personale si trova a operare nelle peggiori condizioni, quando invece è indispensabile il massimo contributo. È necessario pianificare un'attenta, precisa ed essenziale informazione per consentire a tutti di lavorare con efficacia e serenità);
- promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità.

In condizioni ordinarie il Comitato si riunisce con periodicità almeno annuale, allo scopo di valutare lo stato del progetto di continuità, verificare le criticità, attuare e pianificare le iniziative per il miglioramento continuo del progetto stesso.
In condizioni di emergenza, il Comitato assume il controllo di tutte le operazioni e assume le responsabilità sulle decisioni per affrontare l'emergenza, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.
Per svolgere i propri compiti, il Comitato attiva le altre figure identificate come risorse dell'Unità Locale di Sicurezza, che fa in modo che il Comitato possa disporre di strumenti e competenze per affrontare ogni sua decisione.
Il Comitato deve essere supportato nelle seguenti aree:

- **area logistica**, garantendo supporto per gli spostamenti, gli alloggi, ecc.;
- **area tecnologica**, al fine di garantire il funzionamento e l'accesso a tutte le infrastrutture informatiche e di telecomunicazioni predisposte;
- **area informazioni**, tramite aggiornamento di tutte le notizie provenienti dai canali pubblici di comunicazione;
- **area comunicazioni di processo**, tramite raccolta di tutti i rapporti di stato dai vari gruppi di lavoro.

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

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

Si rammenta, comunque, la necessità per le Amministrazioni di rispettare, nella complessiva definizione della politica di CO dell'ente, gli adempimenti imposti dal quadro normativo vigente in materia di protezione dei dati personali (DLgs.. 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 della privacy.

4.3 Funzioni del Gruppo Di Supporto

L'Amministrazione può valutare la possibilità di costituire apposito Gruppo di supporto alle attività del Comitato di gestione della crisi, cui potrà essere affidata la responsabilità – nella gestione ordinaria – delle seguenti funzioni:

- redazione del piano di continuità operativa e proposta al Comitato di gestione per l'approvazione;
- gestione e manutenzione del piano di continuità operativa (compreso l'aggiornamento dei riferimenti interni del personale);
- adeguamento periodico dell'analisi di impatto (BIA);
- studio di scenari di emergenza e definizione delle strategie di rientro;
- gestione dei rapporti con le assicurazioni;
- attuazione delle attività di divulgazione e di sensibilizzazione interna sui temi della continuità;
- tutte le funzioni che il Comitato vorrà delegare.

Dovendo offrire supporto su più temi, questo Gruppo dovrà essere costituito da esperti di gestione del patrimonio tecnologico, di risorse umane, di formazione, di logistica, di supporto amministrativo, di rapporti con i fornitori.
In condizioni di emergenza, il Gruppo di supporto è responsabile del coordinamento gestionale delle attività e di relazione sullo stato delle stesse al Comitato. Il Comitato e il Gruppo di supporto, in caso di necessità, si riuniscono presso un apposito sito di direzione delle operazioni.
Laddove l'Amministrazione non istituisca detto Gruppo, le attività e i compiti descritti nel presente paragrafo rimarranno in capo al Comitato di gestione della Crisi (di cui al precedente paragrafo 5.2)

4.4 Criteri e Indicazioni Organizzative

In generale, nell'ambito delle problematiche legate alla creazione e gestione di una soluzione di continuità, una particolare attenzione deve essere riservata al coinvolgimento del personale interno, soprattutto nei casi in cui la gestione delle infrastrutture informatiche sia di competenza, in tutto o in parte, di personale interno all'amministrazione e non affidata in outsourcing a società esterne.
Si richiama la necessità assoluta di predisporre e aggiornare periodicamente elenchi di riferimenti per tutte le persone coinvolte nelle attività di gestione dell'emergenza e ripristino, individuando chiaramente e controllando chi è tenuto a effettuare queste attività. Ovviamente tali elenchi hanno elevato carattere di riservatezza, contenendo anche informazioni personali.
Allo scopo di non instaurare un clima di conflittualità sia nelle fasi di avvio e sviluppo del progetto sia, a maggior ragione, nelle fasi ben più importanti di esercizio a regime, è opportuno stabilire alcuni principi fondamentali sia nei confronti del personale interno, sia nei confronti del fornitore. Tali principi vengono espressi nei paragrafi seguenti.

4.5 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 programmatici per la sicurezza dovuti a termine di legge, 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 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.

4.5.1. Scopo

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

4.5.2. 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

4.5.3. 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 (Documento Programmatico della Sicurezza (DPS); Piano di Continuità Operativa (PCO); 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.

4.5.4. Responsabilità

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

4.5.5. Verifica salvataggi

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

4.5.6. Lista dei dati salvati

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

4.5.7. 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 (DPS, 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.

4.5.8 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

4.5.9 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.

4.6 Indicazioni per l'avvio della realizzazione di una soluzione di continuità operativa o Disaster Recovery (CO/DR)

È buona prassi, sin dalla fase di avvio del progetto per la realizzazione di una soluzione di CO/DR coinvolgere il personale addetto alla gestione delle infrastrutture, chiarendo nel modo più dettagliato possibile la ripartizione dei compiti tra fornitore e amministrazione.
Occorre inoltre che il personale dell'amministrazione si senta protagonista dell'intera operazione. Quindi, i dirigenti debbono illustrare le motivazioni, non solo tecniche, che sono alla base della soluzione scelta.

Nella fase di avvio e realizzazione delle soluzioni di CO/DR occorre infine sensibilizzare anche le funzioni esterne all'area informatica (organizzazione, gestione del personale, organi tecnici quali ingegneri e avvocati, ecc.) in quanto tali funzioni saranno interessate alla stesura e all'approvazione del Piano che costituirà il documento essenziale per la corretta gestione della continuità.

4.7 Indicazioni per il collaudo e per i test di verifica periodica dell'adeguatezza della soluzione

Si ricorda che, come si avrà modo di precisare anche nel successivo capitolo 6 che attiene più prettamente ai suggerimenti e agli strumenti giuridici e operativi, l'avvio di una soluzione di continuità operativa deve essere obbligatoriamente seguito in ogni caso da attività di verifica di conformità e collaudo, sia se la realizzazione viene attuata all'interno dell'Amministrazione, sia se viene affidata, parzialmente o totalmente, ad un fornitore esterno.
L'Amministrazione dovrà verificare, attraverso apposito collaudo, l'adeguatezza e funzionalità della soluzione adottata e, nel caso di realizzazione affidata a un fornitore esterno, detto collaudo dovrà essere effettuato secondo modalità contrattualmente previste.
Il superamento del collaudo (come si avrà modo di precisare sempre nel successivo capitolo 6) è indispensabile non solo per il pagamento dei servizi resi, ma anche ai fini dell'effettivo avvio del servizio.
Al termine del collaudo deve essere compilato un dettagliato verbale, da sottoscrivere in contradditorio, per certificarne l'esito, che dovrà riportare almeno: la data, l'ora, il luogo dello svolgimento del collaudo, le figure che vi hanno partecipato, le prove svolte e l'esito.

Le Amministrazioni dovranno in ogni caso effettuare test di verifica periodica dell'adeguatezza della soluzione, cercando di riprodurre nel modo più dettagliato possibile il verificarsi di un'emergenza reale e registrando gli esiti del test e le eventuali azioni da effettuare ove il test abbia avuto esito negativo.
Ove le attività di gestione e manutenzione di una soluzione siano effettuate ricorrendo ad un fornitore esterno al termine del test deve essere compilato un dettagliato verbale, da sottoscrivere in contraddittorio, per certificarne l'esito, che dovrà riportare almeno: la data, l'ora, il luogo dello svolgimento del test, le figure che vi hanno partecipato, le prove svolte e l'esito.
In caso di insuccesso parziale o totale dei test, l'Amministrazione deve esaminare le problematiche emerse e attivare le azioni necessarie per la loro risoluzione.
In tal caso il verbale dei risultati dei test dovrà indicare le azioni da intraprendere per la rimozione degli eventuali problemi riscontrati nel corso dei test unitamente alla persona o struttura incaricata di rimuoverli e alla scadenza prevista.

È buona prassi conservare con le modalità di legge il verbale di collaudo e quelli relativi ai test periodici svolti, fino al termine di vigenza della soluzione di continuità operativa e o del contratto che affida ad un fornitore l'avvio, la realizzazione, la gestione e la manutenzione e verifica/test della soluzione.

4.8 Indicazioni per Il Piano di Continuità Operativa

In fase di stesura del Piano di CO (tenuto conto del *template* indicativo minimo, descritto nel successivo capitolo 7) occorre risolvere tutte le problematiche relative all'impegno di personale interno all'amministrazione, con riferimento non solo al personale tecnico IT, ma a tutte le funzioni

coinvolte nell'erogazione dei servizi critici, ivi compreso il personale addetto alla gestione delle applicazioni.
L'emergenza potrebbe infatti modificare in tutto o in parte gli abituali aspetti organizzativi e logistici, con la conseguente necessità di operare in modalità completamente diverse da quella ordinaria.
Potrebbe ad esempio essere necessario cambiare la sede di lavoro, utilizzare procedure diverse per la gestione delle applicazioni, informare gli utenti esterni ed interni sull'impossibilità di fornire alcuni servizi o fornirli comunque in maniera ridotta.
Occorre quindi concordare con il personale e con le RSU sindacali tutte le procedure straordinarie che rendano possibile la continuità dei servizi critici.
Occorre, almeno:

- definire dettagliatamente ruoli e responsabilità di tutti gli attori;
- concordare la gestione della reperibilità del personale in qualunque orario;
- concordare le procedure alternative con le quali erogare i servizi essenziali.

È indispensabile, infine, che tutto quanto concordato ai punti precedenti sia approvato ai massimi livelli dell'amministrazione e che le procedure organizzative definite siano continuamente aggiornate e comunicate a quanti dovranno gestire l'emergenza.

Le Amministrazioni devono poi definire il Piano di Disaster Recovery, che è parte integrante del Piano di Continuità operativa.

Si ricorda peraltro che l'art. 50 bis del CAD affida alle Amministrazioni il compito di *verificare la funzionalità del piano di continuità operativa con cadenza biennale* e che nello stesso articolo si prevede la verifica annuale del costante aggiornamento dei piani di Disaster Recovery delle amministrazioni interessate.

4.9 Indicazioni per la gestione e la manutenzione della soluzione di CO/DR e del Piano di CO/DR

Dal punto di vista organizzativo, è buona prassi che la gestione della soluzione di continuità operativa preveda una serie di riunioni ordinarie e di riunioni straordinarie dei vari gruppi di lavoro coinvolti. Ad esempio, è necessario indire delle periodiche riunioni ordinarie del Comitato di gestione della crisi o del Gruppo di supporto (se presente), con lo scopo di:

- verificare la rispondenza dei Piani di CO/DR alle esigenze dell'amministrazione;
- pianificare i test di verifica dell'adeguatezza della soluzione e del Piano di CO/DR;
- verificare la validità dei test stessi a prove ultimate;
- analizzare le cause dei major incident per valutare eventuali adeguamenti o miglioramenti del piano di CO/DR

È opportuno indire riunioni ordinarie con frequenza semestrale, eventualmente anche precedenti il periodo previsto per i test, in modo da consentirne una corretta e precisa pianificazione. Inoltre possono essere riconvocate dopo i test, qualora questi non abbiano avuto esito positivo.
Copia del resoconto della riunione ordinaria deve essere distribuita almeno a:

- tutti i componenti del Comitato di gestione;
- tutti i componenti del Gruppo di supporto, se presente;

È compito del responsabile del Gruppo verificare che le non conformità evidenziate dalla valutazione della check-list e i problemi evidenziati nei test di manutenzione ordinaria siano rimossi nei tempi previsti. I verbali delle riunioni di manutenzione ordinaria devono essere archiviati in formato magnetico e cartaceo presso la segreteria di progetto.
La riunione straordinaria, viceversa, è il meccanismo attraverso il quale il Comitato di gestione e il Gruppo di supporto (se presente) recepiscono i cambiamenti organizzativi dell'amministrazione, i cambiamenti tecnici del sistema informativo e di quant'altro possa esercitare un impatto sostanziale sulla struttura e/o sul contenuto del Piano.
Le riunioni straordinarie, a causa della loro tipologia, non possono avere una frequenza prestabilita. La loro convocazione, in caso di necessità, è demandata al responsabile del Gruppo di supporto.

4.10 Indicazioni per la documentazione

Come già detto precedentemente, per assicurarsi che la soluzione di continuità sia perfettamente funzionante in caso di necessità, è fondamentale che la documentazione sia disponibile in ogni momento, sia mantenuta sempre aggiornata e che le versioni successive dei manuali vengano distribuite in modo corretto agli interessati.
Ogni modifica a uno qualsiasi dei documenti che costituiscono il Piano, siano essi manuali o allegati esterni, ne comporterà una variazione di modifica e/o release.
Una modifica a un manuale o a un allegato esterno che scaturisca da una manutenzione ordinaria darà luogo a una nuova release del documento (passerà da m.n a m.n+1). Una modifica a un manuale o a un allegato esterno che scaturisca da una manutenzione straordinaria darà luogo a una nuova versione del documento (passerà da m.n a m+1.0). Dovranno essere aggiornati di conseguenza i dati di controllo presenti nella copertina del documento, la versione nel piè di pagina e la data nell'intestazione.
A ogni nuova versione o release di uno dei documenti che costituiscono il Piano sarà creata una nuova versione o release dell'allegato esterno "Indice dei documenti" contenente gli estremi delle ultime versioni o release modificate.
La copia cartacea delle nuove versioni o release dovrà essere firmata per approvazione sulla copertina dal responsabile del Gruppo di supporto unitamente alla data di approvazione. Dopo la firma, dovrà essere aggiornata la copia magnetica inserendo il nome del responsabile del Gruppo di supporto e la data di approvazione, e archiviato il documento in formato magnetico/cartaceo secondo lo standard definito.
A ogni nuova versione/release dei documenti che costituiscono il Piano, ha il compito di curare la distribuzione dello stesso affinché le "copie ufficiali" del Piano siano sempre aggiornate.

Ai fini dell'invio degli studi di fattibilità tecnica a DigitPA e per facilitare l'identificazione delle strutture da coinvolgere nella realizzazione del piano, si riporta di seguito una scheda per l'individuazione delle responsabilità della singola Amministrazione e dei punti di contatto interni previsti a livello (eventuale) di Aree Organizzative o di Enti dipendenti dall'Amministrazione.
Il Dirigente identificato come responsabile della CO si farà carico della realizzazione del Piano, nonché dell'invio a DigitPA di un unico Studio di Fattibilità per tutte le entità dipendenti.

Nome Amministrazione		
Sede centrale		
Settore attività		
Responsabile CO		
1	AOO (area organizzativa omogenea) / Ente	
	Punto di contatto	
	Indirizzo PEC per le comunicazioni	
	Data compilazione	
2	AOO (area organizzativa omogenea) / Ente	
	Punto di contatto	
	Indirizzo PEC per le comunicazioni	
	Data compilazione	
n	AOO (area organizzativa omogenea) / Ente	
	Punto di contatto	
	Indirizzo PEC per le comunicazioni	
	Data compilazione	

5 LA REALIZZAZIONE DELLA CONTINUITÀ OPERATIVA E DELLE SOLUZIONI DI DISASTER RECOVERY NELLE PA

5.1 Determinazione delle esigenze di continuità e delle soluzioni

Ferma restando la necessità per le Amministrazioni di assicurare la Continuità dei servizi ICT, tenuto conto degli aspetti delineati nei precedenti capitoli, di regola non è possibile individuare la soluzione di CO/DR più opportuna senza una preventiva analisi delle conseguenze dei possibili 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 A al presente documento) per condurre ad una stima da parte dell'Amministrazione delle tolleranze 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 al DigitPA 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 uno specifico profilo tra quelli previsti. A ciascuno dei profili, i quali sono definiti 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 a DigitPA.

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 DLgs.. 196/2003 (contenente le disposizioni del "Codice in materia di Protezione dei dati personali") e s.m.i.;

- delle regole tecniche che sono in corso di emanazione da parte di DigitPA 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, come si avrà modo di evidenziare nel successivo capitolo 7, saranno inviati a DigitPA, in formato elettronico, in allegato allo Studio di Fattibilità Tecnica.

5.2 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 (percorsi meglio descritti, come detto, nella già citata appendice A al presente documento), al fine di coadiuvare le Amministrazioni ad ottemperare, nei tempi previsti agli obblighi previsti dall'art. 50-bis del CAD, si è ipotizzato 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 potrà essere di supporto il *template* riportato nel paragrafo 7.1.

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.

5.2.1 Le direttrici di analisi

Gli indicatori che tipicamente sintetizzano le esigenze di continuità operativa sono, come già discusso, RTO e RPO. Tali valori vengono generalmente individuati a seguito di un'analisi di impatto (BIA) che, valutando le criticità dei servizi, fornisce una stima relativamente ai valori tollerabili di tempi di fermo e di quantità di dati persi in seguito ad incidente o disastro.

Data la complessità delle diverse realtà delle PA, e la difficoltà di individuare per ognuna di esse i valori puntuali dei suddetti parametri, ai fini del presenti Linee Guida si è optato per l'adozione di uno strumento di supporto semplificato all'autovalutazione e all'analisi quali-quantitiva. Per evitare tuttavia di incorrere in soluzioni troppo semplicistiche, quali quelle che in prima approssimazione inferiscono i valori di RTO ed RPO dalla mera complessità organizzativa dell'Amministrazione (adottando l'ipotesi semplificativa che a complessità crescenti corrispondano necessariamente servizi più critici), si è proceduto ad individuare uno strumento di valutazione multidimensionale che porti in conto non una sola caratteristica, quale ad esempio la semplice dimensioni della struttura IT, ma un set più completo di informazioni che coprano innanzitutto la criticità dei servizi erogati, a cui si aggiungono la complessità dell'organizzazione dell'Amministrazione e quella della struttura IT che abilita alla erogazione dei servizi. Ciò in quanto non è detto che una Amministrazione dotata di molti apparati abbia necessariamente delle esigenze più stringenti rispetto ad una che ne abbia pochi.

La stima sulla criticità dei servizi viene pertanto 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.

5.2.2 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 successivo paragrafo 0.

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 privacy;
- numero dei trattamenti censiti nel DPS;
- numerosità degli addetti tramite i quali vengono erogati i servizi;
- numerosità degli utenti esterni.

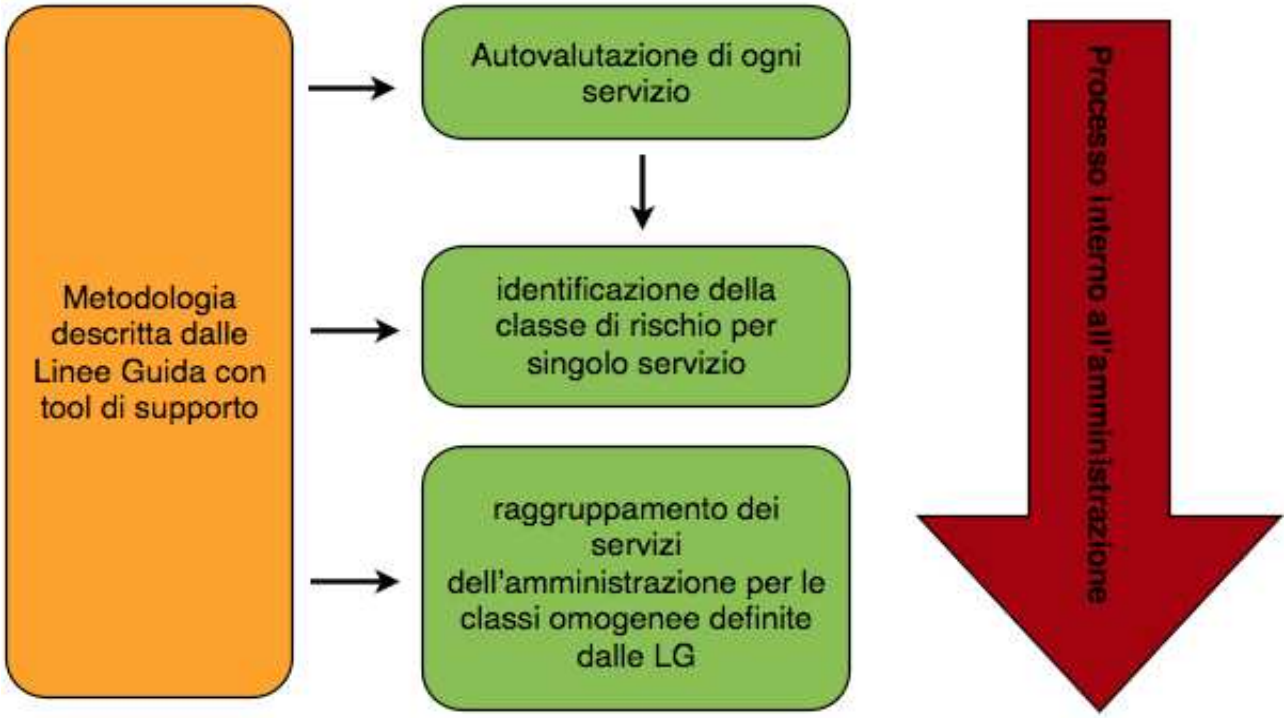
Con riguardo alla direttrice della *tecnologia* i criteri identificati sono:

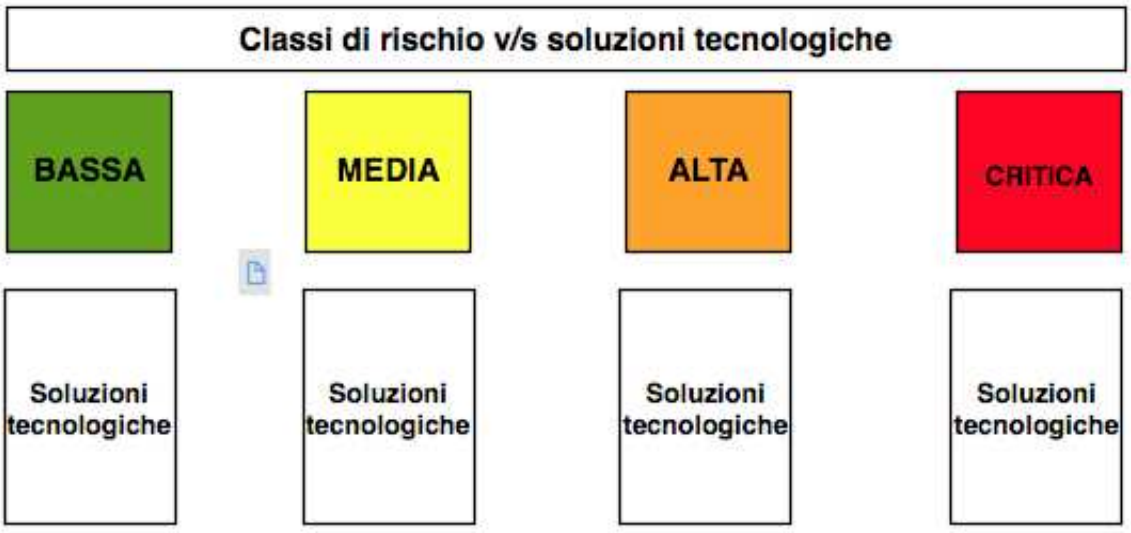
- presenza di un dipartimento IT;
- numerosità addetti IT;
- architettura elaborativa;
- architettura applicativa;
- numero di server;
- numero di postazioni di lavoro;

- 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.

Lo schema sottostante sintetizza l'intero processo definito.





5.2.3 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 DLgs. 196/03 e s.m.i. ("Testo unico in materia di protezione dei dati personali") 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 su 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 coerenza dei dati ed esistere un'unica copia storage;
- la disponibilità dei dispositivi (storage su 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.

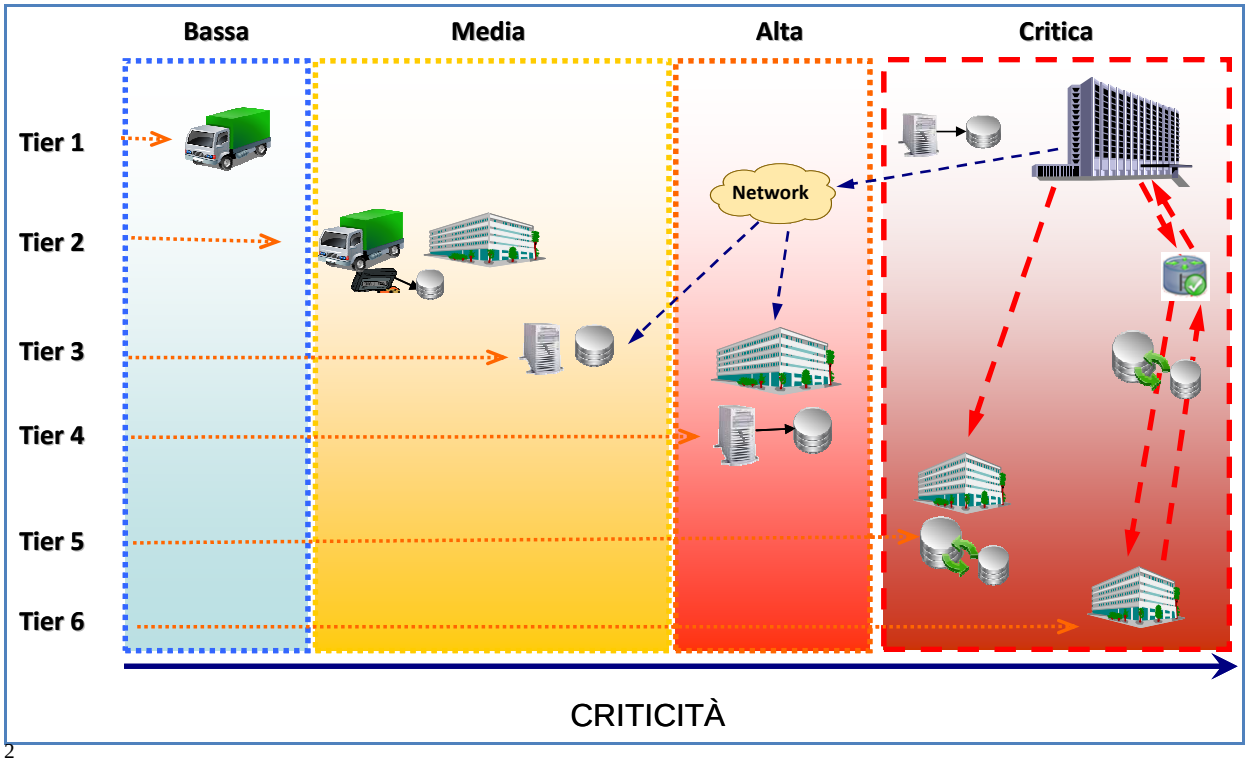
***Tier 3**:* la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario 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).

***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. 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.

***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.

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



[2]

5.3 *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; la periodicità del salvataggio; il tipo di salvataggio (totale/incrementale); le modalità di conservazione (come accennato nel precedente capitolo 4).
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;

[2] I tier presentati tengono conto del disposto normativo che impone, comunque, la disponibilità di un sito alternativo, per assicurare, a fronte di emergenze, il ripristino dei servizi. Peraltro, anche ove l'RTO scelto sia dell'ordine di giorni, è possibile adottare soluzioni atte a garantire una perdita dei dati contenuta (da zero minuti a poche ore). Inoltre, non è escluso che soluzioni che prevedano più siti alternativi (ad es. un sito secondario di BC o in balancing col sito primario e un ulteriore sito che svolge effettivamente il ruolo di sito alternativo di DR) possano non trovare perfetta corrispondenza nei tier di massima individuati, potendo, ad es., la soluzione di BC corrispondere, per indici e valori di RTO e RPO, ad un determinato tier e il vero e proprio sito di DR riconoscersi nelle soluzioni tecniche e nei valori di RPO e di RTO di un altro tier.

- se e come il servizio erogato dal sito secondario abbia le stesse caratteristiche di quello primario.

5.3.1 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.

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

Soluzioni tecnologiche basate su virtualizzazione o 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/DR.

5.3.2.1 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/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.

5.3.2.2 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 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 accedovi tramite Internet (*Public cloud*) o tramite intranet private (*Private cloud*).

L'utilizzo di servizi in modalità cloud permette 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.

La tipologia più nota è sicuramente quella definita come "*Public cloud"* ovvero 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 la gestione di determinati servizi implica, infatti, il trattamento di dati da parte di outsourcer che spesso hanno sede in stati diversi soggetti a giurisdizioni diverse.

Alcuni importanti fornitori di servizi *cloud*, infatti, non comunicano l'esatta locazione geografica dei dati gestiti in quanto, per le caratteristiche stesse della tecnologia in questione, gli stessi 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).

La situazione non sempre migliora affidandosi ad un fornitore che garantisca la localizzazione geografica dei dati in quanto, salvo rare eccezioni, solitamente i servizi sono situati al di fuori dell'Unione Europea. Col 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.

Scegliendo opportunamente fornitori e clausole contrattuali e/o accordi di servizio, anche servizi di tipo cloud possono essere opportunamente progettati e regolamentati secondo le esigenze delle Amministrazioni. Come si avrà modo di ricordare nel capitolo 6, il Codice della Privacy (DLgs. 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 del citato DLgs. 196/2003 e s.m.i. che regola il "Trasferimento dei dati all'estero").

Al riguardo nella scelta di soluzioni che comportano il trasferimento dei dati, come avviene attraverso le soluzioni *cloud*, è necessario tener presente 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 della Privacy 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.

Si ritiene altresì opportuno in materia la consultazione del 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".
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 dei dati gestiti.

5.3.2.3 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 che, sulla base delle modalità di backup individuate, 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, 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.

5.4 Lo strumento di supporto per l'autovalutazione

In appendice C viene illustrato il modello matematico messo a punto per l'autovalutazione secondo i criteri generali descritti nei precedenti paragrafi.

6 STRUMENTI GIURIDICI E OPERATIVI PER L'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, procedono alla sua realizzazione attraverso l'acquisizione delle necessarie infrastrutture e dei servizi.
Anche le Amministrazioni che saranno in grado di progettare e realizzare una soluzione organizzata e gestita internamente dovranno, verosimilmente, procedere all'acquisizione delle infrastrutture tecnologiche e delle risorse software necessarie a rendere operativi i piani di CO/DR adottati. Nello specifico, sarà necessario per tutte le Amministrazioni destinatarie delle prescrizioni contenute nel CAD, acquisire non solo apparati hardware e tecnologie software ma, anche, locali attrezzati e servizi di comunicazione dedicati.
Le metodologie e le soluzioni di CO/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 continuità operativa e Disaster Recovery 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, allora, saranno presentate delle casistiche di ricorso al mercato per l'adempimento degli obblighi imposti dal CAD e una serie di requisiti minimi e opzionali per la stipula dei contratti di fornitura dei servizi necessari all'attuazione della continuità operativa (CO/DR).

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

Il conferimento da parte di una pubblica amministrazione, ad 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 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";
- DLgs.. 12 aprile 2006, n. 163: "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 (Gazz. Uff. 30 dicembre 1997, n. 302): "Regolamento recante approvazione del capitolato di cui all'articolo 12, comma 1, del DLgs.. 12 febbraio 1993, n. 39, relativo alla locazione e all'acquisto di apparecchiature informatiche, nonché alla licenza d'uso dei programmi";

- La legge 12 luglio 2011, n. 106 di "Conversione in legge, con modificazioni, del decreto-legge 13 maggio 2011, n. 70", concernente "Semestre Europeo. Prime disposizioni urgenti per l'economia".

6.1.1 Il dialogo competitivo

Laddove l'Amministrazione, che deve pur dare attuazione all'art. 50-bis del CAD, non sia oggettivamente in grado di definire, i mezzi tecnici atti a soddisfare le sue necessità o i suoi obiettivi, né sia oggettivamente in grado di specificare l'impostazione giuridica o finanziaria del progetto che intende avviare per dotarsi di una soluzione di continuità, può provare a ricorrere alla procedura del dialogo competitivo prevista dall'art. 58 del DLgs..163/2006 e s.m.i. e dal relativo Regolamento di attuazione.
L'Amministrazione può ricorrervi quando l'appalto che intende affidare sia particolarmente complesso, e qualora ritenga che il ricorso alla procedura aperta o ristretta non permetta l'aggiudicazione dell'appalto.
Possono, secondo le circostanze concrete, essere considerati particolarmente complessi gli appalti per i quali la stazione appaltante non dispone, a causa di fattori oggettivi ad essa non imputabili, di studi in merito alla identificazione e quantificazione dei propri bisogni o all'individuazione dei mezzi strumentali al soddisfacimento dei predetti bisogni, alle caratteristiche funzionali, tecniche, gestionali ed economico-finanziarie degli stessi e all'analisi dello stato di fatto e di diritto di ogni intervento nelle sue eventuali componenti.
La procedura non può essere utilizzata in modo abusivo o in modo da ostacolare, limitare o distorcere la concorrenza.
L'unico criterio per l'aggiudicazione dell'appalto è quello dell'offerta economicamente più vantaggiosa.

L'Amministrazione che intende utilizzare il dialogo competitivo procederà 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 Informatico, i servizi, le applicazioni e i dati che intende ricoverare, 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, definendo 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) e i criteri di valutazione delle offerte (di cui all'articolo 83, comma 2) e il termine entro il quale gli interessati possono presentare istanza di partecipazione alla procedura;
- avviare la fase di preselezione delle imprese che presentando domanda di partecipazione, invitandole a presentare proposte tecniche (e non economiche), avviando con i candidati ammessi un dialogo finalizzato all'individuazione e alla definizione delle soluzioni e 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.

6.1.2 I principi della Strategia Lisbona e il "Green Public Procurement" (GPP)

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 c.d. "strategia di Lisbona" per la crescita e l'occupazione che sin dal 2000 ha identificato nella sostenibilità ambientale uno dei pilastri della competitività europea, promuovendo misure per addivenire ad acquisti sostenibili;
- 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 DLgs.. 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*".

6.1.3 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 che attiene agli "*Appalti pubblici e accordi quadro stipulati da centrali di committenza*" prevede che:

"*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, comma 1, lettere b), c), f), 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".

Le centrali di committenza possono stipulare convenzioni, contratti o accordi quadro.
Al riguardo si segnala che anche in ambito regionale si possono avviare iniziative di questo tipo; si ritiene opportuno citare il caso della Regione Toscana ove apposita Legge regionale (la n. 38 del 13 luglio 2007) ha disciplinato, nel rispetto del DLgs.. 163/2006, i contratti pubblici di appalto aventi ad oggetto lavori, forniture e servizi eseguiti sul territorio regionale toscano, promuovendo sostanzialmente progetti tesi a ridurre, aggregare e qualificare le stazioni appaltanti, attraverso azioni volte a:

- favorire ed incentivare l'esercizio associato da parte degli enti locali delle funzioni amministrative e dei servizi in materia contrattuale;
- prevedere la possibilità di avvalimento da parte delle amministrazioni pubbliche degli uffici di altre amministrazioni;
- prevedere la possibilità di stipula di apposite convenzioni da parte delle amministrazioni aggiudicatrici per la gestione in comune di procedure di gara.

In particolare, in forza della normativa citata, la Regione per appalti di forniture e servizi che possono rivestire interesse generale per le amministrazioni pubbliche può assumere le funzioni di centrale di committenza. La Regione aggiudica gli appalti di interesse generale: per conto esclusivo, o congiuntamente, degli enti locali, degli enti dipendenti dalla Regione e degli altri enti di cui all'articolo 1, comma 455, della legge 27 dicembre 2006, n. 296 ("legge finanziaria 2007").

6.1.4 Le acquisizioni di beni e servizi tramite Convenzioni e Accordi Quadro Consip

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 delle Convenzioni stipulate da Consip ai sensi dell'art. 26 della L. 488 del 23 dicembre 1999; le singole Amministrazioni, infatti, possono perfezionare ordinativi di fornitura, entro il massimale economico e i quantitativi previsti nelle convenzione medesime.

I recenti adeguamenti normativi introdotti dalla Legge n. 191/09 del 23 dicembre 2009 (Finanziaria 2010, pubblicata in G.U. il 30 dicembre 2009 ed in vigore dal 1° gennaio 2010) attribuiscono 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.

6.1.5 Ulteriori aspetti da considerare

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. 50-bis comma 4 del Codice dell'Amministrazione Digitale impegna le Amministrazioni a definire piani di continuità operativa e di Disaster Recovery sulla base di appositi e dettagliati studi di fattibilità