DigitPA

LINEE GUIDA PER IL DISASTER RECOVERY DELLE PUBBLICHE AMMINISTRAZIONI

ai sensi del comma 3, lettera b) dell'art. 50-bis del DLgs. N. 82/2005 e s.m.i.

BREVE GUIDA ALLA LETTURA

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

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

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

I contenuti delle Linee Guida sono i seguenti:

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

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

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

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

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

Hanno partecipato alle attività del Gruppo di lavoro:

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

Glossario delle principali definizioni utilizzate nel documento

Nell'ambito del presente documento si intende per:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 OBIETTIVI E SCENARI DELLA CONTINUITÀ OPERATIVA DELLE PUBBLICHE AMMINISTRAZIONI

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

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

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

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

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

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

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

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

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

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

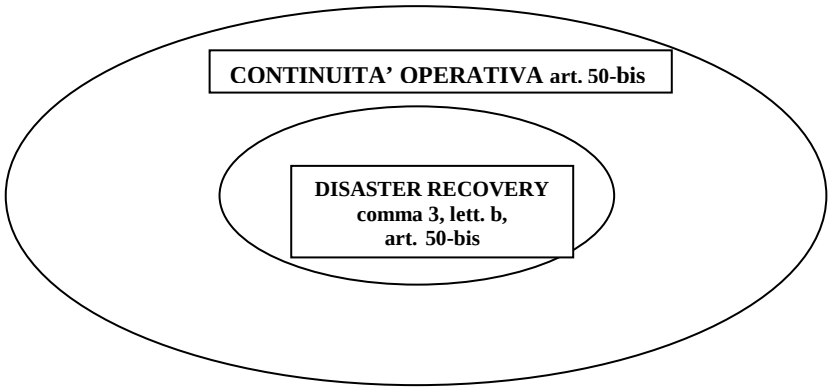
Per continuità operativa ICT - ai sensi e per le finalità di queste linee guida - si intende la capacità di un organizzazione di adottare, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative, misure di reazione e risposta ad eventi imprevisti che possono compromettere, anche parzialmente,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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

La crescente complessità delle attività legate alla Pubblica Amministrazione, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio, quali quelli determinati da un attacco di tipo terroristico o anche solamente malevolo, così come gli inconvenienti di natura tecnica, che possono portare all'interruzione totale dei servizi istituzionali anche per lunghi periodi, evidenziano l'esigenza che le amministrazioni aggiornino il livello di predisposizione a questi potenziali fermi della propria operatività.
In questa direzione, è quindi necessario che le pubbliche amministrazioni adeguino e rafforzino le strategie in tema di sicurezza in modo da garantire la continuità di funzionamento dei sistemi informativi attraverso i quali le stesse Pubbliche Amministrazioni assicurano lo svolgimento dei rispettivi compiti istituzionali e l'erogazione dei servizi all'utenza.
Le pubbliche amministrazioni devono quindi dotarsi nella gestione corrente dei propri servizi ICT, di strumenti, accorgimenti e procedure per assicurare la Continuità Operativa (CO), per poter far fronte a incidenti di ampia portata o a eventi imprevisti che possono comportare l'indisponibilità del proprio Sistema Informativo, al fine di evitare fermi o gravi interruzioni della propria operatività con impatti negativi o disservizi nei procedimenti svolti e nei servizi erogati all'utenza.
L'attuazione della continuità operativa risulta quindi un adempimento inderogabile, tenuto anche conto delle disposizioni in tema di dematerializzazione e conservazione, quali, in particolare, gli articoli di seguito riportati:

Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni
1.Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.

Art. 43. Riproduzione e conservazione dei documenti
1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.
2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.
3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71.
4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42.

Art. 44. Requisiti per la conservazione dei documenti informatici
1. Il sistema di conservazione dei documenti informatici assicura:
a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
b) l'integrità del documento;
c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi ì dati di registrazione e di classificazione originari;
d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.
1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.
1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

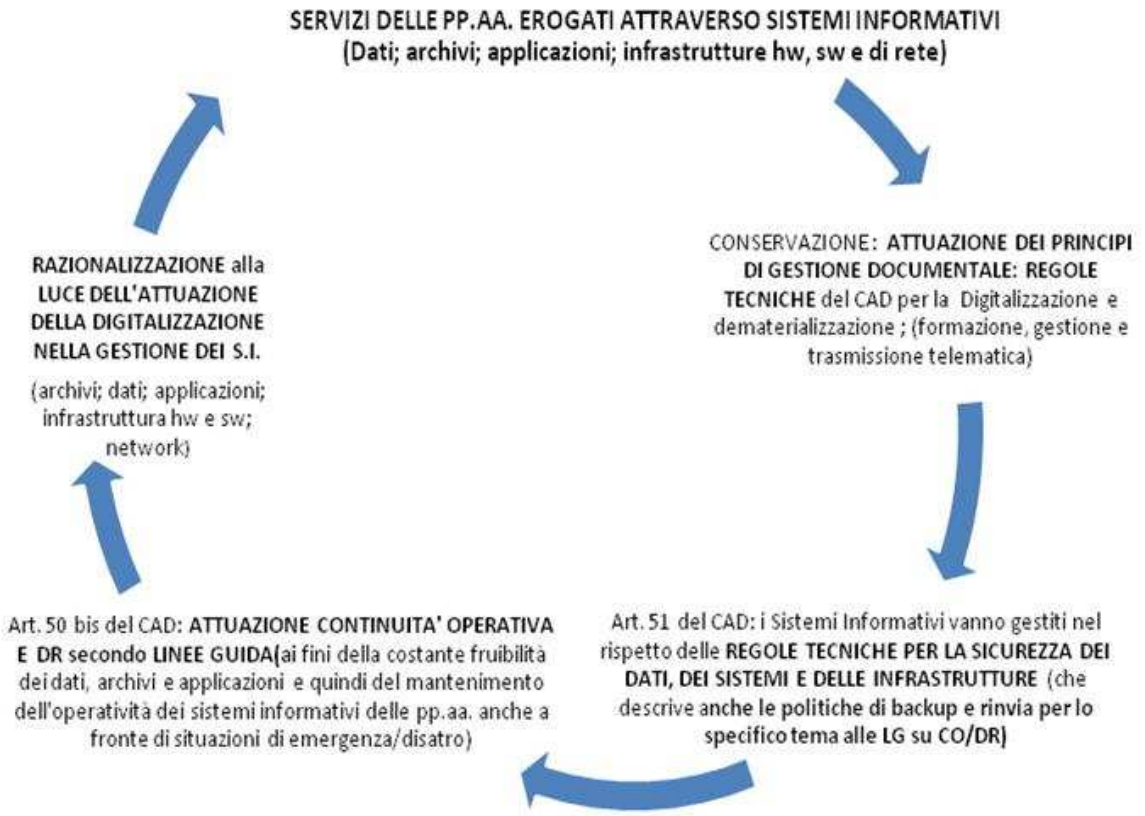
In questo scenario generale la continuità dei sistemi informativi rappresenta per le pubbliche amministrazioni, nell'ambito delle politiche generali per la continuità operativa dell'ente, un aspetto necessario all'erogazione dei servizi a cittadini e imprese e diviene uno strumento utile per assicurare la continuità dei servizi e garantire il corretto svolgimento della vita nel Paese.

Al riguardo e più in particolare l'articolo 50-bis del CAD aggiornato (che attiene alla "Continuità operativa") delinea gli obblighi, gli adempimenti e i compiti che spettano alle Pubbliche Amministrazioni, a DigitPA e al Ministro per la pubblica amministrazione e l'innovazione, ai fini dell'attuazione della continuità operativa:
1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le p.p.a.a. predispongono i

piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio e il ritorno alla normale operatività.
2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.
3. A tali fini, le pubbliche amministrazioni definiscono:
a. il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;
b. il piano di Disaster Recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di Disaster Recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.
4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.".

Nell'articolo 2 dello stesso CAD, così come innovato dal citato DLgs.. 235/2010, in merito alle finalità e all'ambito di applicazione si prevede peraltro quanto segue:
"Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.
2. Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311 (…)
5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

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



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

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

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

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

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

- **a DigitaPA il compito di**:
  - definire, sentito il Garante per la protezione dei dati personali, le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche;
  - verificare annualmente il costante aggiornamento dei Piani di DR delle amministrazioni interessate;
  - informare annualmente il Ministro per la pubblica amministrazione e l'innovazione;
  - esprimere pareri sugli studi di fattibilità che le amministrazioni predispongono e sulla base dei quali provvederanno a definire sia il piano di continuità operativa che il piano di DR.

- **alle Amministrazioni il compito** di definire in prima battuta gli studi di fattibilità e sulla base di detti studi - entro quindici mesi dall'entrata in vigore del DLgs 235/2010 - i piani di emergenza, continuità operativa e Disaster Recover.

- **al Ministro per la pubblica Amministrazione e l'innovazione** il compito di:
  - assicurare l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni;
  - informare con cadenza annuale Il Parlamento.

- **alle Regioni ed alle Provincie autonome il compito** di:
  - avviare al proprio interno il medesimo percorso di attuazione dell'art.50-*bis* del CAD;
  - promuovere le iniziative necessarie a generare la consapevolezza sulle specifiche necessità di CO e DR, all'interno degli enti territoriali minori, anche facilitando il percorso di realizzazione da parte delle singole realtà;
  - diffondere le presenti linee guida, quale strumento di agevolazione per la definizione e l'adozione dei piani di CO e DR da parte degli enti territoriali minori.

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

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

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

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

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

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

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

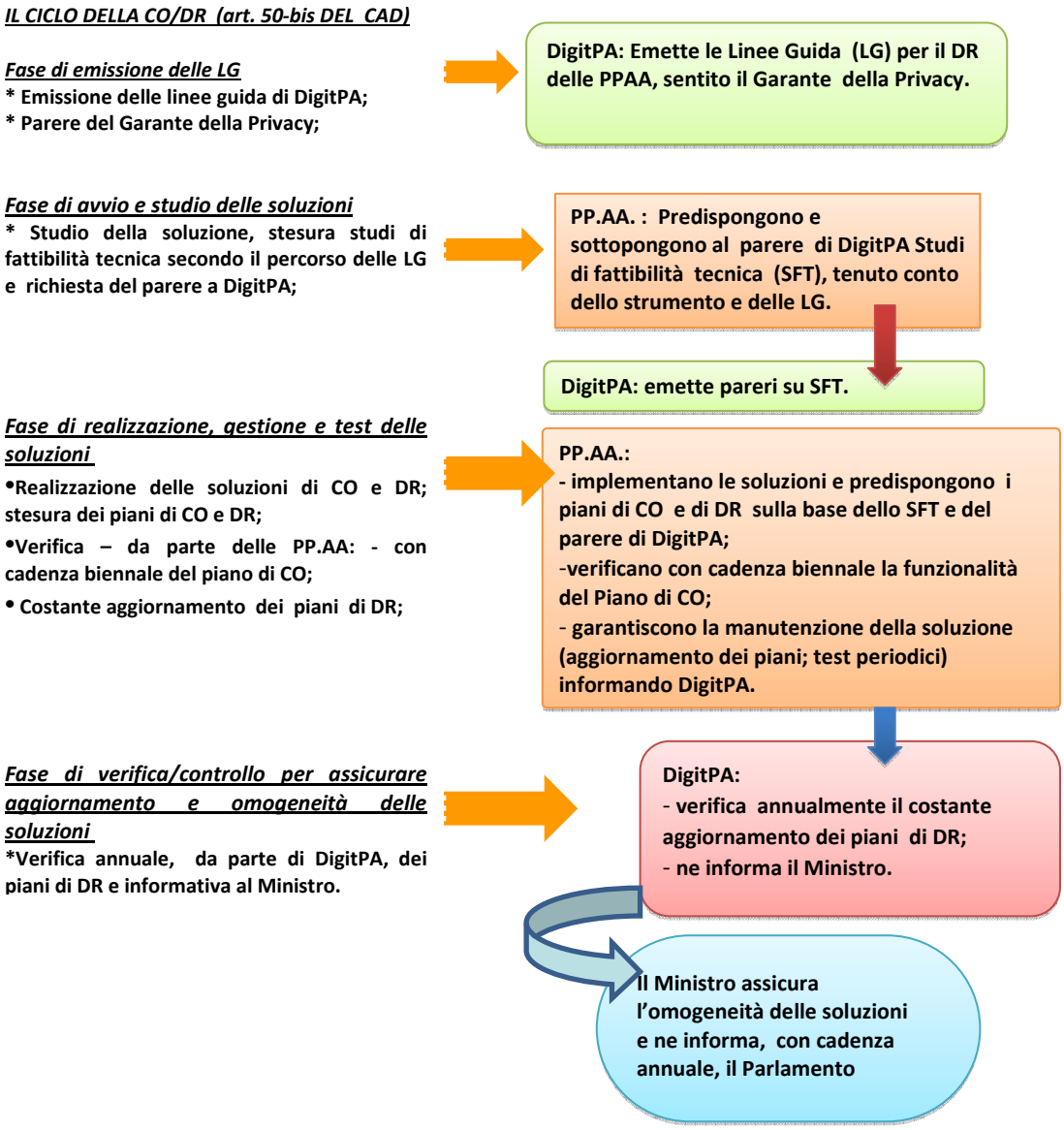
Inoltre, per consentire a DigitPA di verificare annualmente il costante aggiornamento dei piani di Disaster recovery delle Amministrazioni e informare il Ministro per la pubblica amministrazione e l'innovazione, le Amministrazioni dovranno inviare a DigitPA i piani di Disaster Recovery, e devono verificare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

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

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

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

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



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

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

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

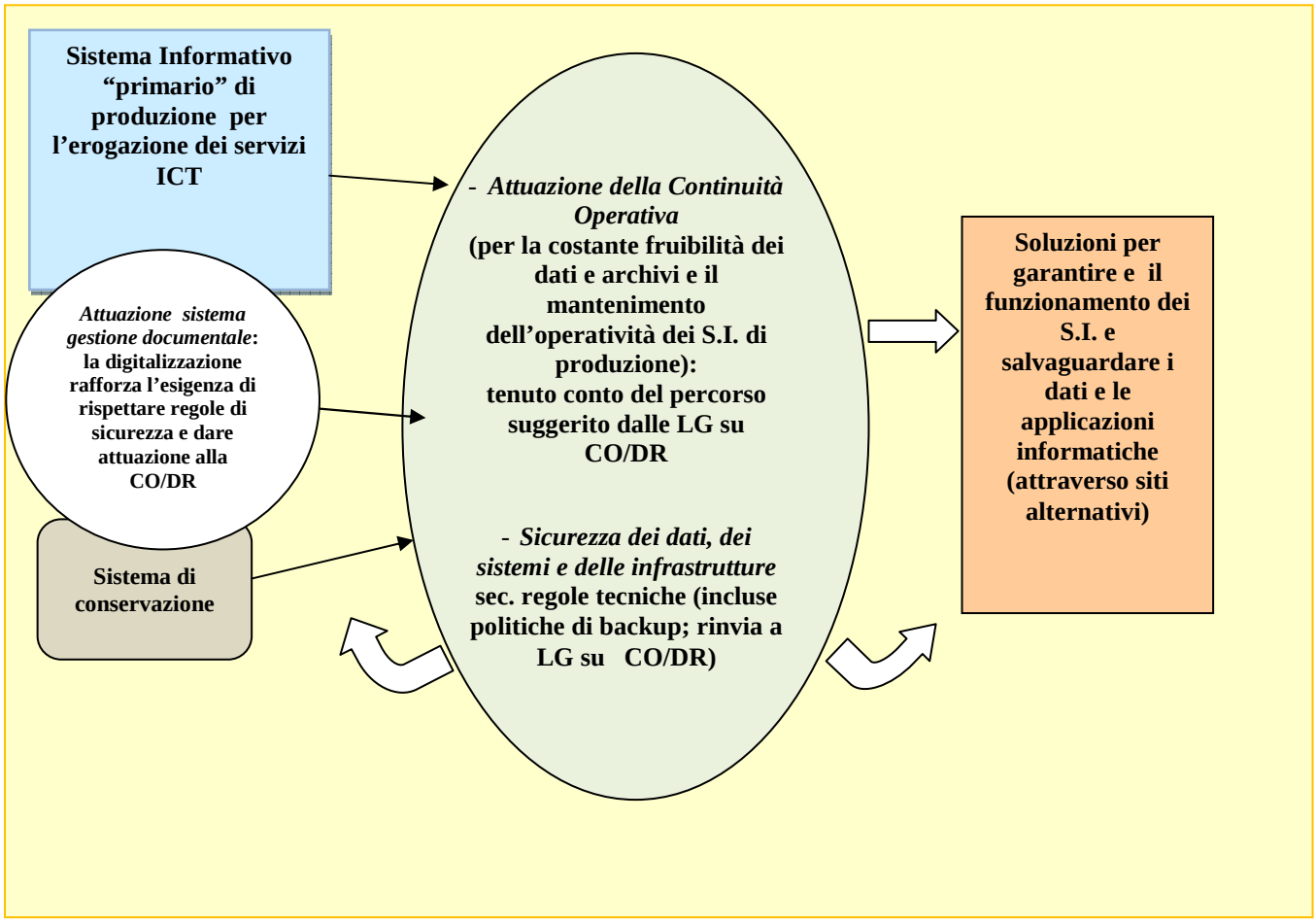
Il secondo comma del richiamato articolo 51 conferma altresì, come si è avuto modo di anticipare, che" *I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non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

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

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

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

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


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

3 STANDARD DI RIFERIMENTO PER L'ATTUAZIONE DELLA CONTINUITÀ OPERATIVA

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

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

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

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

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

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

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

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

3.1 Standard internazionali

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

3.2 Standard di tipo "buone pratiche"

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

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

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

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

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

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

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

3.3 La base di conoscenza del DRII

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

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

Questo quadro di riferimento è riconosciuto internazionalmente.

3.4 Lo standard BS 25999

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

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

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

3.4.1 BS 25999-1 e BS 25999-2

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

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

3.4.2 I sei punti del BS 25999-1

Lo standard evidenzia principalmente sei punti:

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

3.5 Lo standard BS 25777

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

3.6 I lavori dell'ISO

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

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 contradditorio, 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.

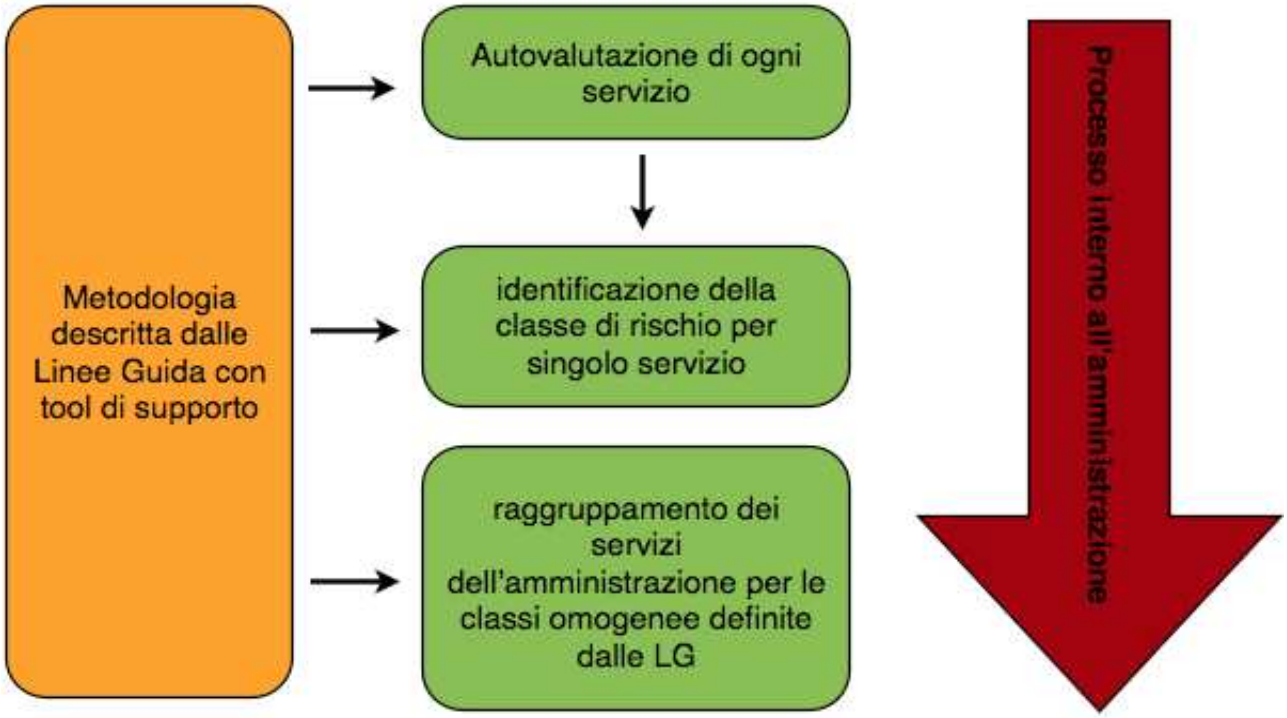
Con riguardo alla direttrice della *tecnologia* i criteri identificati sono:

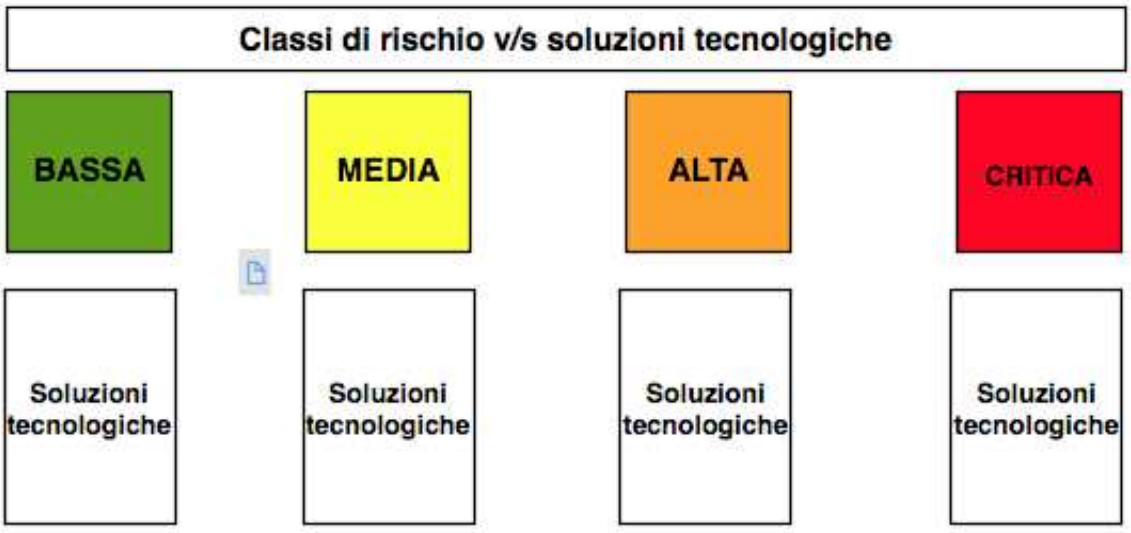
- presenza di un dipartimento IT;
- numerosità addetti IT;
- architettura elaborativa;
- architettura applicativa;
- numero di server;
- numero di postazioni di lavoro;

- 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.

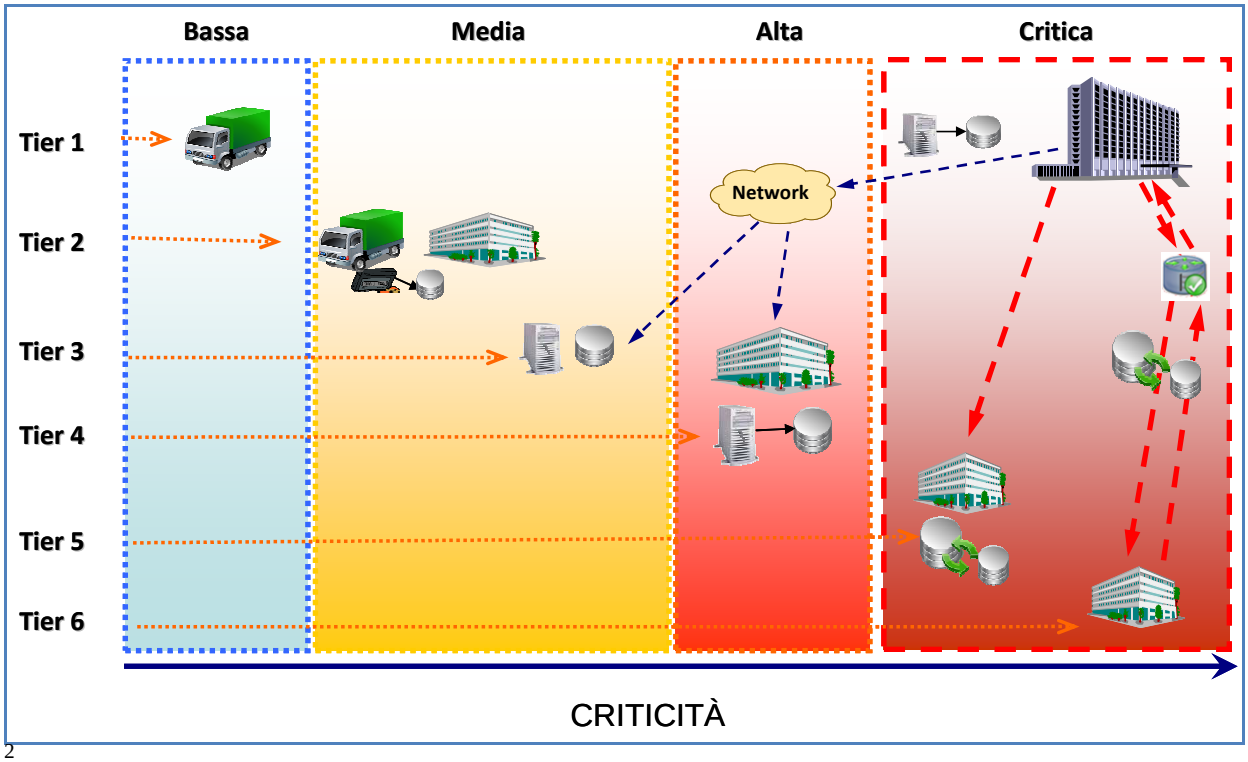
***Tier 3**:* la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario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

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.50-bis, nonché l'obbligo ex artt. 9 e 17, comma 2, DLgs 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.

6.2 La realizzazione di soluzioni di continuità operativa

Nella realizzazione delle soluzioni di CO/DR le Amministrazioni possono, in linea di massima, 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 DLgs. 196/03 ("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) 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

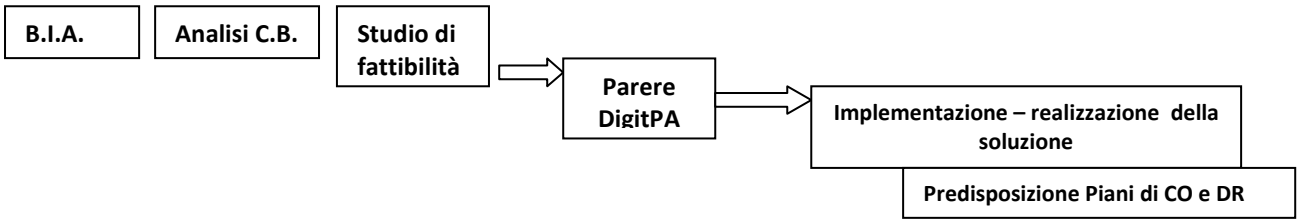
rendano necessario, sempre all'Amministrazione "mutuata", la presenza di personale in orari di chiusura dell'Amministrazione "mutuante").

I servizi che si possono richiedere per l'attuazione di una soluzione di CO/DR sono di seguito schematicamente descritti nelle linee generali: la composizione dei beni e servizi che possono dover essere acquisiti da una Pubblica Amministrazione 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 percorsi per l'acquisizione delle soluzioni di CO/DR.
Nei casi in cui una Amministrazione debba dotarsi di una soluzione di CO/DR e non disponga, in tutto o in parte, al proprio interno 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/DR, attuando, ad esempio i percorsi descritti nelle ipotesi di seguito riportate.

6.2.1 Ipotesi A: progettazione e implementazione di una soluzione di CO/DR da parte dell'amministrazione

In questo caso l'amm.ne 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.

Ipotesi A: l'intero processo è interno all'Amministrazione



6.2.2 Ipotesi B: progettazione di una soluzione di CO/DR da parte di un fornitore

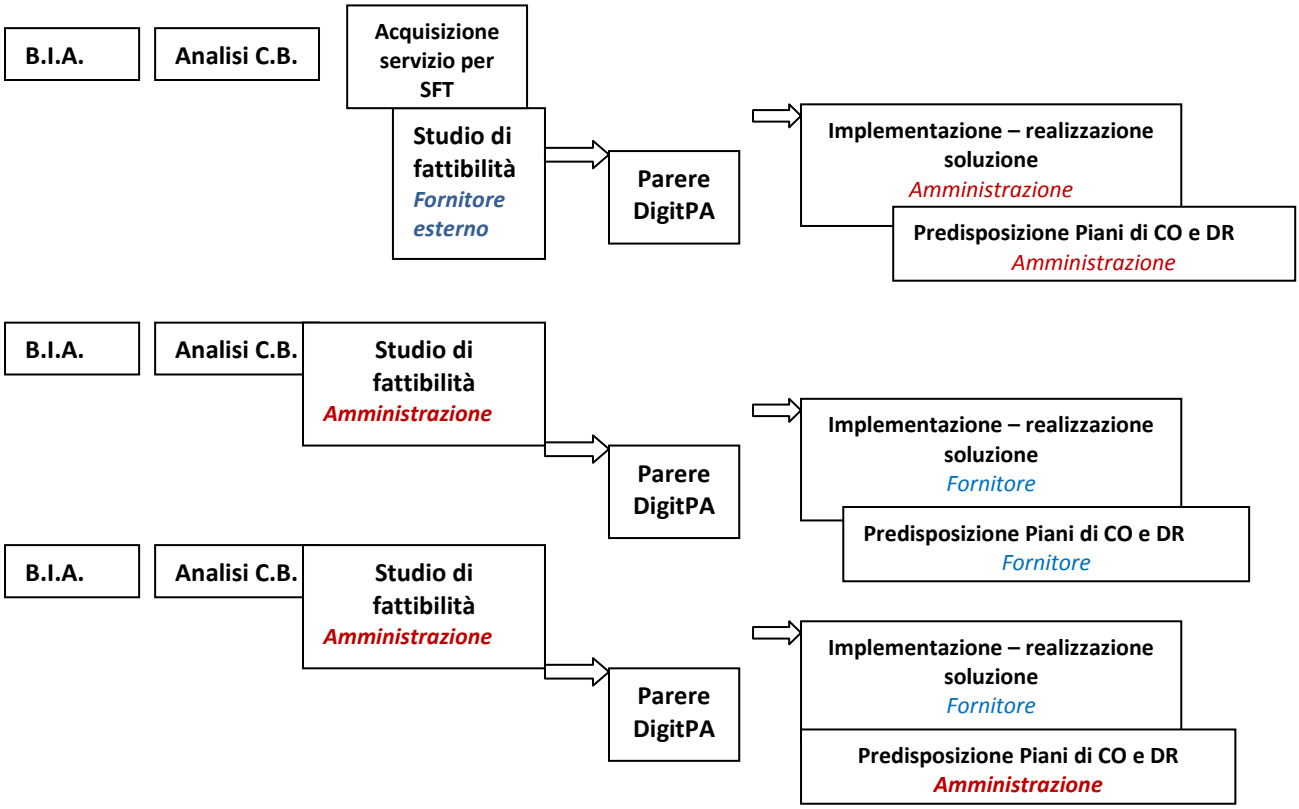
Di tutta evidenza, in questo caso, la necessità di una preliminare ed accurata ricognizione del contesto tecnico che connota il Sistema Informativo primario per il quale deve essere progettata la soluzione.
Al termine della fase di ricognizione si ritiene opportuno che il fornitore fornisca apposito 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, al Documento programmatico della sicurezza ex DLgs.. 196/2003, 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

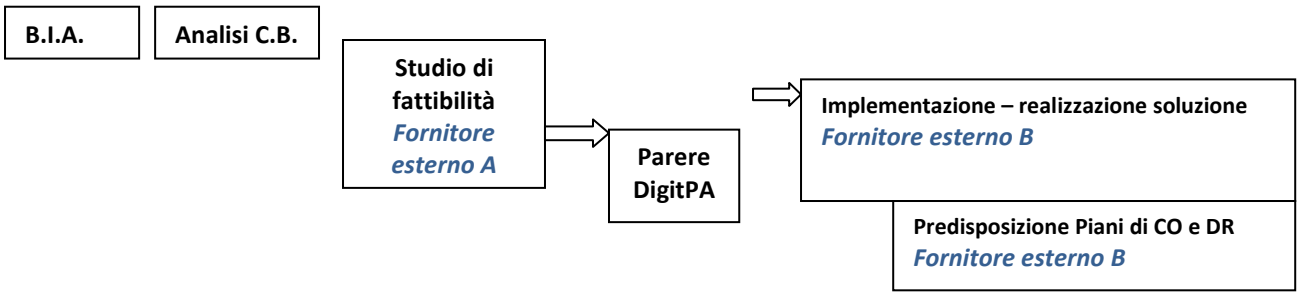
Ipotesi B: il processo è svolto dall'Amministrazione con l'acquisizione di parte del servizio (tre esempi)



6.2.3 Ipotesi C: progettazione e realizzazione di una soluzione di CO/DR da parte di 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 Il mutuo soccorso

Come si è avuto modo di accennare, nella realizzazione delle soluzioni di CO/DR le organizzazioni possono anche assumere impegni di assistenza volontaria, stipulando un accordo di mutuo soccorso e offrendosi 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.
Le condizioni che favoriscono l'adozione di soluzioni basate su accordi di mutuo soccorso sono:

- la comunanza di compiti;
- l'esistenza di problematiche di continuità analoghe e non particolarmente stringenti;
- la presenza di sistemi informativi con dimensioni e architetture simili;
- la 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 di mutuo soccorso 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.

In merito alle soluzioni di mutuo soccorso senza la pretesa di esser esaustivi si segnalano le seguenti due possibilità, rimandando per quanto attiene alle considerazioni relative agli aspetti tecnici, al precedente capitolo 5.

6.2.5 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. Per questo motivo gli accordi di mutuo soccorso tra organizzazioni indipendenti non sono molto frequenti e, di regola, non coinvolgono più di due organizzazioni.
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.
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.

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 o protocolli di intesa tra amministrazioni e organismi responsabili dell'erogazione di servizi ritenuti fondamentali. In tal caso, l'ente terzo può essere parte attiva nella definizione dei piani d'emergenza e nel coordinamento delle attività di soccorso.

6.2.6 Accordi tra strutture di una stessa organizzazione

Sono possibili accordi di mutua assistenza 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 elaborative.
L'accordo è quasi sempre di tipo multilaterale: la struttura centrale ha il compito di redigere un modello di piano di continuità operativa e uno schema di accordo che sia valido per tutta l'organizzazione. Ciascuna struttura aderente all'accordo dovrà personalizzare il piano di continuità operativa in funzione delle proprie specificità ed esigenze e dovrà predisporre le risorse occorrenti per eventuali attività di soccorso. Nel caso in cui un'emergenza coinvolga più strutture, normalmente la struttura centrale svolge il ruolo di coordinamento dei soccorsi.

6.3 I possibili servizi da richiedere per l'attuazione di soluzioni di continuità operativa ICT e Disaster Recovery

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.

I servizi che si possono richiedere 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.

6.3.1 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 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 della Privacy 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. Al proposito, si ricorda anche 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.

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.

6.3.2 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 l'osservanza delle specifiche tecniche e dei vincoli previsti dalla normativa vigente (fra cui, ad esempio: il DLgs. 9 aprile 2008, n. 81 di "Attuazione dell'art. 1 della 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 DLgs. 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).

Aspetti da tenere in considerazione quando si deve costruire o scegliere un datacenter sono 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.

6.4 Possibili servizi 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 (DLgs.. 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.

6.5 Le eventuali prestazioni da richiedere 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.

6.5.1 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).

6.5.2 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.

6.6 Cenni sugli aspetti di connettività

Le soluzioni di Disaster Recovery possono prevedere una componente di rete per la connettività tra centro primario e sito alternativo. Si ricorda che nel caso di centro primario gestito da un fornitore, e non direttamente dall'Amministrazione, è necessario inserire come vincolo contrattuale al fornitore del centro 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.

6.7 Cenni agli strumenti e clausole da adottare per soluzioni tecniche (cloud) che implichino il trasferimento dei dati (rinvio alla normativa comunitaria e ai provvedimenti del Garante della Privacy)

Per quanto attiene alle soluzioni cloud, si osserva quanto segue.
Come si è già avuto modo di evidenziare nel capitolo 5, nel caso di 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 della Privacy (DLgs.. 196/2003 e s.m.i.), 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 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, comma 2;
e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 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, comma 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;
h) il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

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), dall'altro sottolineando le proprie perplessità in relazione a questa tecnologia ed evidenziando l'obsolescenza della normativa attualmente vigente rispetto al mutato scenario tecnologico.

Si ricorda, altresì, che nella definizione degli schemi contrattuali connessi a 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.

In questo panorama 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.

6.8 Strumenti, clausole e disposizioni di carattere generale

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 DLgs.. 231/01 e dalla successiva Direttiva Comunitaria relativa, definendo anche quanto previsto dalla legge 136/2006, così come modificata dal D.L. del 12 novembre 2010, n. 187 in materia di tracciabilità dei flussi finanziari e prevedendo la nullità o risoluzione di diritto a fronte di inadempimenti agli obblighi previsti (le Amministrazioni potranno tener conto al riguardo anche delle determinazione dell'Autorità per la vigilanza sui contratti pubblici n. 8 del 18 novembre 2010 e n. 10 del 22 dicembre 2010).
Come si è avuto modo di anticipare, 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.

E' necessario anche prevedere clausole:

- che regolino l'obbligo di riservatezza e gli obblighi del fornitore di improntare il proprio operato a quanto previsto dal DLgs.. 196/2003 e s.m.i. "Codice in materia di protezione dei dati personali", in particolare, individuando esplicitamente, ai sensi del Titolo IV 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 della Privacy, personalizzato anche sulla base delle misure di sicurezza e del DPS dell'Amministrazione; al proposito, si ricorda anche 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;
- 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; n.b. verifica DUVRI; Dlgs. 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.

7 LO STUDIO DI FATTIBILITÀ TECNICA E I PIANI PER LA CO E IL DR DELLE PA

Data la crescente importanza della continuità operativa dei sistemi informativi delle Pubbliche Amministrazioni, è stata colta l'occasione della revisione del CAD per inserire in tale revisione un nuovo articolo, il 50-bis "Continuità operativa", l'unico nella revisione che non riprenda disposizioni già presenti nel vecchio testo e che è specificamente rivolto a questo importante aspetto.

Come si è già avuto modo di evidenziare nel capitolo 2 del presente documento l'articolo prevede:

- la predisposizione di un piano di continuità (comma 3, punto a), inclusivo del piano di Disaster recovery (comma 3, punto b), da parte di tutte le pubbliche amministrazioni (come identificate all'articolo 2 del CAD stesso);
- la stesura, preventiva al precedente adempimento, di un apposito studio di fattibilità, sul quale deve essere obbligatoriamente richiesto parere a DigitPA (comma 4).

Si ritiene che lo Studio di Fattibilità Tecnica (SFT) debba contenere, a grandi linee, l'esito del processo di autovalutazione (vedi sopra) e la sintesi dei seguenti aspetti, nonché le iniziative attuate o che si intendono realizzare per ottemperare agli impegni previsti dal CAD, con evidenza, ove necessario (es. non esistenza di piani e soluzioni di DR) dei tempi stimati e del percorso previsto per garantire l'aderenza al CAD.

7.1 Lo Studio di Fattibilità Tecnica

In questo paragrafo si illustra il modello di riferimento di massima che dovrà essere utilizzato per la compilazione dello SFT che l'Amministrazione deve sottoporre a DigitPA, al termine della fase di autovalutazione eseguita, secondo quanto illustrato nel precedente capitolo 5, con il supporto del foglio elettronico o tool analogo reso disponibile da DigitPA. Il documento di SFT serve a dare evidenza dei risultati emersi dalla fase di autovalutazione, illustrando anche:

- gli eventuali scostamenti tra la soluzione individuata all'esito del percorso di autovalutazione e quella effettivamente scelta dalla Amministrazione;
- il percorso e i tempi che l'Amministrazione stima siano necessari per adottare la soluzione suggerita all'esito del percorso di autovalutazione e per allinearsi alle presenti Linee Guida.

Lo SFT deve essere compilato dalla singola Amministrazione e presentato dal "Responsabile della Continuità Operativa" (di cui si è trattato nel precedente capitolo 4). Nel caso di una Amministrazione articolata in diverse strutture che operano sostanzialmente in modo autonomo, si dovrà avere sempre un unico SFT. Eventualmente, per facilità di presentazione, la suddivisione in capitoli di seguito proposta potrà essere ripetuta per ogni struttura dell'Amministrazione. L'adozione di questa scelta deve essere esplicitata nel documento.
Le tabelle e gli esiti del percorso di autovalutazione, come si è già avuto modi di evidenziare nel capitolo 5, vanno inviati a DigitPA, in formato elettronico, in allegato allo Studio di Fattibilità Tecnica.

Fatte queste premesse, i contenuti minimi di uno SFT possono essere organizzati come indicato di seguito.

a) INFORMAZIONI GENERALI

In questo paragrafo vanno riportate le informazioni generali dell'Amministrazione che emette lo SFT. Le informazioni sono le stesse richieste dallo strumento di autovalutazione (e già descritte nel precedente capitolo 5 del presente documento).

b) L'AMBITO DELLO STUDIO DI FATTIBILITÀ TECNICA

In questo paragrafo 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 tecnica per la continuità operativa ICT e DR.
È 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.

Va riportato l'elenco dei servizi o delle classi di servizi (gli stessi per cui è stata fatta l'autovalutazione):

- servizio/ classe di servizi 1
- servizio/ classe di servizi 2
- …
- servizio/ classe di servizi N

Per ogni servizio/classe di servizi in allegato allo SFT vanno riportate in dettaglio le tabelle compilate in fase di autovalutazione.

c) IL RISULTATO DEL PERCORSO DI AUTOVALUTAZIONE

In questo paragrafo, per ogni servizio/classe di servizi che fa parte dell'ambito dello Studio di Fattibilità Tecnica tenuto conto del percorso descritto nel precedente capitolo 5, devono essere riportati i dati emersi nel corso dell'autovalutazione e che sono riportati nello schema di sintesi dell'autovalutazione, ossia:

- indice complessivo di criticità;
- classe di criticità;
- soluzione tecnologica.

d) LA SOLUZIONE TECNICA

In questo paragrafo deve essere indicato se i servizi o classe di servizi in ambito allo SFT sono coperti da un'unica soluzione o sono previste diverse soluzioni. In quest'ultimo caso deve essere riportata una mappa di copertura tra le singole soluzioni e i servizi.

Se le soluzioni effettivamente adottate differiscono da quelle suggerite dal risultato dell'autovalutazione, è necessario riportarne in dettaglio le motivazioni.
Nel caso in cui lo SFT comprenda più soluzioni, per ognuna di esse deve essere compilato un paragrafo in cui riportare:

Soluzione X (X indica il numero della soluzione)

In questo sottoparagrafo deve essere riportato a quale servizio/classe di servizi si riferisce la soluzione. La soluzione dovrebbe essere una delle sei tipologie di soluzione descritte nel capitolo 5 delle presenti Linee Guida.

Architettura soluzione X (X indica il numero della soluzione)
In questo sottoparagrafo deve essere descritta l'architettura tecnica ed applicativa che si intende adottare per la soluzione X, avuto riguardo a tutto quanto attiene al perimetro della Continuità Operativa ICT delineato nel capitolo 1 delle LG.

e) TEMPI E MODALITÀ DI REALIZZAZIONE DELLA SOLUZIONE

In questo paragrafo per il complesso delle soluzioni riportate nel SFT, devono essere riportati i tempi e le modalità di realizzazione delle soluzioni individuate, fermo restando che, come si è avuto modo di evidenziare nel precedente capitolo 6 (e salve restando le situazioni particolari che non lo rendano possibile, per vincoli tecnici oggettivi), 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.

Inoltre 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.
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 è avuto modo di accennare in precedenza nel presente documento, dovrà quindi 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.

7.2 Il Piano di Continuità Operativa

Preliminarmente va tenuto presente che sotto la dizione "piano di continuità operativa" possono essere rappresentati insieme documentali molto differenti: per una realtà di dimensioni limitate, soprattutto sotto il profilo ICT, il PCO (che deve sempre prevedere una componente dedicata al Disaster Recovery) può essere un unico documento. 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 e finanche documenti di terzo livello, per esempio sotto la forma di istruzioni di lavoro che riportano le indicazioni operative specifiche.

Fatta questa premessa, è possibile sintetizzare per il PCO i seguenti contenuti minimi:

a) ***FINALITÀ E AMBITO DI APPLICAZIONE***.
   Lo scopo e la portata di ogni piano dovrebbe essere definito, concordato dai vertici dell'Amministrazione e adeguatamente compreso da coloro che dovranno, all'occorrenza, attuarlo a tutti i livelli. In questo settore del PCO vanno indicati:

   - i servizi da recuperare e le priorità di recupero;
   - il tempi entro i quali i servizi devono essere recuperati (RTO);
   - i livelli di recupero necessario per ogni servizio (RPO);

- le condizioni che portano a invocare il piano.

b) RUOLI E RESPONSABILITÀ.
I ruoli (a cominciare dal responsabile della continuità operativa) e le responsabilità delle persone e del (dei) team (si veda al riguardo il precedente capitolo 4) che sono coinvolti, in termini di processo decisionale e di livello di autorità durante e dopo un'emergenza devono essere chiaramente documentati.

c) MODALITÀ DI ATTIVAZIONE, GESTIONE E MANUTENZIONE DEL PCO.
Va premesso che il tempo perduto nel decidere di attivare la risposta a una situazione di emergenza deve essere considerato come irrecuperabile. Quindi, è sempre meglio attivare una risposta all'emergenza iniziando una risposta ICT piuttosto che perdere l'occasione di contenere l'emergenza e prevenire una escalation di conseguenze. Le modalità con cui viene attivato il PCO devono essere chiaramente documentate. Perciò, il piano dovrebbe includere in una descrizione chiara e precisa:

- le modalità per mobilitare le persone e i team interessati;
- la localizzazione dei punti di ritrovo;
- le circostanze in cui l'organizzazione ritiene che l'attivazione del PCO non sia necessaria (ad esempio, guasti di entità minore, magari anche a rischio di superamento delle soglie di tolleranza all'interruzione, ma che possono essere recuperati in tempi rapidi: va infatti valutato che attivare una condizione di risposta all'emergenza implicherà, al termine dell'emergenza stessa, un periodo dedicato al rientro alla normalità, che può rivelarsi non semplice e, soprattutto, non rapido);
- le modalità di gestione, manutenzione e verifica e test del PCO;
- il piano di Disaster Recovery, come documento a sé stante, o, nei casi più semplici, direttamente descritto nel PCO (si veda in dettaglio nel successivo capitolo);
- le modalità di rientro dall'emergenza (per esempio, in un contesto ICT, il retro-allineamento dei dati elaborati in fase di emergenza con quelli del centro primario).

Infine, l'Amministrazione dovrebbe anche identificare chi ha l'incarico di curare tutte le revisioni al PCO, da gestire con un adeguato sistema di controllo delle versioni, e di dare le correlate informazione a tutte le parti interessate. Infine, vanno anche previste le modalità di comunicazione (verso le utenze esterne e/o interne).

7.3 Il Piano di Disaster Recovery

I contenuti minimi di un PDR possono essere sintetizzati come nel seguito.

a)INTRODUZIONE
In questo punto devono essere illustrate brevemente le finalità e i contenuti del Piano di Disaster Recovery.

b)DESCRIZIONE DELLA SOLUZIONE DI DISASTER RECOVERY

In questo punto deve essere brevemente descritta la soluzione di Disaster Recovery adottata per assicurare la continuità di funzionamento dei sistemi e ambienti del SI primario a fronte di eventi disastrosi o indisponibilità che colpiscano lo stesso Sistema rendendolo indisponibile.

c)OBIETTIVI DEL PIANO DI DISASTER RECOVERY (PIANO DI DR)

In questo punto deve essere descritto l'obiettivo del piano.
Obiettivo principale del PDR è quello di pianificare le attività connesse alla gestione e manutenzione della soluzione di Disaster Recovery per assicurare sia in condizioni di emergenza, sia per il rientro alla normalità, con riattivazione del/dei Sistema/i Informativo/i Primario/i, al fine di assicurare il ripristino dell'infrastruttura ICT:

- con un RTO massimo di XX giorni solari;
- con un RPO di XX ore su sottosistemi storage a disco con copia remota dei dati o per dati a nastro che provengono da operazioni di backup.

d)INFORMAZIONI RELATIVE AL PIANO DI DR

In questa sezione devono essere sinteticamente riportate le informazioni relative al Piano.
Per comodità nella gestione dell'aggiornamento/delle eventuali revisioni del Piano le informazioni possono essere divise in due sezioni: la prima sezione può contenere **le informazioni statiche** (es. le informazioni che rimarranno costanti e non saranno oggetto di revisioni frequenti); la seconda sezione contiene le **informazioni dinamiche** (es. le informazioni che devono essere aggiornate regolarmente al fine di assicurare che il piano rimanga fattibile ed in costante stato di approntamento). Le informazioni dinamiche da ultimo citate sono quelle che maggiormente possono essere connesse alle revisioni/modifiche del Piano di DR che si rendono necessarie al fine di mantenere detto importante Piano aggiornato rispetto ai cambiamenti/alle eventuali variazioni tecnico-organizzative che si verificano nel contesto tecnico-operativo di riferimento dell'Amministrazione.

e)CLAUSOLE E DIRETTIVE APPLICABILI

In questa sezione vanno elencate tutte le norme, le direttive, i riferimenti di standard, le direttive a cui deve far riferimento il Piano di DR.

f)PERIMETRO DI RIFERIMENTO DEL PIANO

Descrizione del sistema informativo primario e dei servizi critici che la soluzione di DR deve garantire

In questo punto vanno precisate le componenti ed i servizi critici del sistema informativo primario (in termini di infrastrutture, applicazioni, procedure, utenti, ecc) che costituiscono l'ambito per il quale deve essere garantita la soluzione di Disaster Recovery e il sito di DR messo a disposizione per consentire il ripristino della funzionalità e l'attivazione del Sistema Informativo primario a fronte di disastri/indisponibilità prolungate.

Fattori critici e di rischio, descrizione dei casi di disastro/indisponibilità prolungata che si intendono affrontare con la soluzione di DR

In questo punto vanno descritti i fattori di rischio ed i problemi che si intendo specificatamente affrontare e circoscrivere attraverso l'erogazione dei servizi connessi alla soluzione di DR richiesta, di cui nel Piano si deve tener conto.
In questo punto vanno descritti i casi di disastro e/o di indisponibilità dei sistemi informativi primari coperti dalla soluzione di DR che rendono necessario attivare il sito di DR e tener conto delle attività e procedure del Piano di DR.

g)ORGANIZZAZIONE E PERSONALE

Organizzazione, ruoli e responsabilità, strutture e personale coinvolto nelle attività.

In questo punto vanno chiariti i ruoli e le responsabilità, descritte le strutture e le figure professionali (con i relativi riferimenti anagrafici, telefonici, ecc..) che sono coinvolte nella gestione e manutenzione della soluzione di Disaster Recovery nonché nella gestione della crisi e nella eventuale permanenza presso il sito di DR in condizione di emergenza, in caso di disastro e/o di indisponibilità prolungata del sistema informativo primario.

In questa sezione va quindi descritta la struttura di riferimento per la gestione della soluzione di DR e delineate le attività e le competenze, prevedendo, in linea di massima almeno le strutture e le modalità di "*alternate"* ed escalation indicate al precedente capitolo 4.

Modalità di attivazione del personale

In questo punto vanno dettagliate le modalità di attivazione del personale sia in condizioni di normale operatività - per assicurare l'assistenza operativa e la gestione della soluzione di DR – sia in condizioni di emergenza/disastro/indisponibilità del sito primario a seguito della formale "Dichiarazione di Disastro" (che permarrà fino al ripristino del Sistema Primario con la formale "Dichiarazione di fine emergenza").

h)POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI

In questo punto vanno descritte le policy e le misure adottate per garantire la sicurezza e la salvaguardia dei dati del sito di DR in tutte le attività e fasi di erogazione dei servizi connessi alla soluzione di Disaster Recovery.

i) FASI DELLA SOLUZIONE DI DISASTER RECOVERY

In questo punto va accuratamente dettagliata la sequenza di attività da effettuare per le fasi di:

- valutazione della situazione di disastro/di crisi/indisponibilità del sito primario;
- dichiarazione del Disastro;
- attivazione del Piano di DR e delle procedure ad esso connesse;
- notifica, informativa ed attivazione delle strutture e del personale coinvolto nelle attività connesse alla dichiarazione di Disastro;
- attivazione del sito di DR e ripristino del sistema informativo primario colpiti dal disastro/dalla situazione di indisponibilità;
- gestione dei sistemi informativi primari presso il sito di DR in condizioni di emergenza, durante il periodo di disastro/Indisponibilità;
- ripristino del Sistema Primario con la formale "Dichiarazione di fine emergenza".

l)GESTIONE DEL PIANO

In questo punto vanno descritte le attività da svolgere per garantire la predisposizione e l'aggiornamento/revisione del Piano di DR, nonché i principali adempimenti per garantire la verifica periodica dell'adeguatezza della soluzione di DR.

m)COLLEGAMENTI/EVENTUALI INTERAZIONI CON GLI ALTRI DELIVERABLE CONTRATTUALI

In questo punto vanno descritti gli eventuali nessi, interazioni e collegamenti con gli altri deliverable previsti (es. documentazione delle procedure; manualistica ecc.)

n)PROCEDURE DI TEST

In questo punto vanno richiamate le modalità di svolgimento e documentazione delle procedure di test periodiche previste per garantire la verifica dell'adeguatezza della soluzione e del Piano di DR, tenuto conto di quanto già suggerito nei precedenti capitoli del presente documento.

8 CONTINUITA' OPERATIVA E DISASTER RECOVERY DELLE INFRASTRUTTURE CRITICHE

8.1 Premessa

Il compito affidato dal CAD a DigitPA 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 quell'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, 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 (DLgs 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*[3] e di *infrastruttura critica*[4], 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.

3 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.

4 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.

8.2 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.

8.3 Le 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 DLgs.. 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 DLgs 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 DLgs 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 DLgs 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 DLgs. 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.

8.4 La PA come IC

Ad oggi la PA non è inclusa nei settori indicati dal DLgs 61/2011 e probabilmente non sarà mai interessata dalla legislazione riguardante le Infrastrutture Critiche Europee in quanto si ritiene che la Pubblica Amministrazione sia una realtà prettamente nazionale e non possa quindi avere ricadute al di fuori dello Stato Membro al quale appartiene.
Tuttavia è molto probabile che la PA sarà interessata dalla eventuale normativa in merito alla individuazione di Infrastrutture Critiche nazionali e da eventuali normative discendenti a livello locale (regionale, provinciale, comunale, ecc.). Ad oggi, come già detto, sono stati elaborati i criteri che dovrebbero essere utilizzati nella direttiva del Presidente sulla individuazione e designazione delle ICN (Infrastrutture Critiche Nazionali), ma la direttiva stessa è ancora in lavorazione.

In attesa di una normativa generale non è ovviamente possibile specificare aspetti di dettaglio riguardanti, in particolare, eventuali obblighi o "migliori pratiche" che dovrebbero essere adottate dalla PA intesa come Infrastruttura Critica.

E' molto probabile che le definizioni e gli aspetti salienti della disciplina delle IC come delineati dalla Direttiva 114/08 CE vengano mutuati anche nell'applicazione nazionale e, forse, anche a livello locale (regionale, provinciale, comunale, a discrezione delle competenti autorità).

Quando la nuova normativa avrà definitivamente individuato gli obiettivi di protezione delle IC (Nazionali, regionali, ecc.), sarà possibile affrontare concretamente aspetti di maggiore dettaglio. Di seguito, viene fornita una lista degli aspetti più rilevanti che dovranno essere affrontati

8.5 La resilienza della PA

Per resilienza di un sistema si suole intendere la capacità del sistema medesimo di rispondere ad un potenziale evento distruttivo mediante una adeguata procedura di ripristino della propria funzionalità e di rientro ad una condizione di operatività predefinita, accettata e sicura.
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.
Come anticipato in premessa, 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. Di seguito si riportano gli elementi che potranno consentire di realizzare la resilienza nella PA italiana:

(A) Definizione di una Best Practice organizzativa
Atteso il ruolo che PA nazionale assumerà nel percorso di identificazione delle infrastrutture critiche nazionali, appare necessario poter definire un modello organizzativo comune per le pubbliche amministrazioni che saranno coinvolte in questo percorso di identificazione delle ICN, direttamente come gestori di infrastrutture critiche o di sistemi ICT interconnessi con

ICN, ovvero indirettamente per il ruolo e la responsabilità che singoli Enti esercitano istituzionalmente nei confronti di altri soggetti pubblici e privati operanti nei settori e sotto-settori identificati per le specifiche necessità di protezione.
Ad integrazione di quanto dettagliatamente rappresentato nel capitolo 4 delle presenti Linee Guida, in relazione alla creazione presso ogni pubblica amministrazione della figura del Responsabile della Continuità Operativa e del Comitato di Gestione della Crisi, si ritiene indispensabile integrare le strutture organizzative esistenti nelle PA, mediante l'istituzione di un Comitato Strategico per la Sicurezza che assicuri una visione unitaria a livello di Amministrazione e sia in grado di valutare sia il rischio operativo complessivo sia le necessarie misure di sicurezza da attuare. Nell'ambito delle infrastrutture critiche, infatti, diviene ancor più necessario poter ricondurre la direzione di tutte le attività pertinenti la sicurezza in un unico centro di competenza apicale, dotato di autonomia e responsabilità, cui affidare il compito di governare la politica di sicurezza ICT dell'Ente e di garantire una centralità di indirizzo ed un coordinamento unitario ed omogeneo per tutte (e solo) quelle amministrazioni che hanno un ruolo di responsabilità nelle infrastrutture critiche nazionali.

Il Comitato strategico per la Sicurezza dovrebbe essere composto da:

- Il Direttore Generale dell'ente o ruolo equiparato
- Il responsabile dell'Ufficio Unico Dirigenziale ex art. 17 del CAD;
- il Responsabile della Continuità Operativa
- Responsabile dell'unità locale di Sicurezza
- Responsabile della Segr. NATO-UEO
- Responsabile Privacy
- Responsabile Pianificazione finanziaria
- Direttore del personale
- Il Responsabile della sicurezza fisica *ex DLgs 81 del 2008*

Al Comitato è demandata la politica di sicurezza dell'ente nel suo complesso (risorse umane, edifici, impianti, infrastrutture ICT, patrimonio informativo) e, se prevista dall'emananda disciplina interna sulle ICN, potrà avere il compito di definire le modalità di interazione con il Nucleo Interministeriale Situazione e Pianificazione (NISP) e con la Segreteria infrastrutture critiche (SIC).

Nelle pubbliche amministrazioni che saranno identificate come titolari di responsabilità diretta o indiretta di infrastrutture critiche nazionali, il Comitato di Sicurezza integrerà e sostituirà il Comitato di Gestione della Crisi, previsto per le altre amministrazioni in attuazione delle presenti Linee Guida (capitolo 4).

(B) Salvaguardia dei dati ed applicazioni: i Piani di continuità operativa e Disaster Recovery

La realizzazione di quanto previsto dall'art.50-bis 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 sarà realizzato e monitorato attraverso il ruolo attribuito a DigitPA, 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 al Ministro per la PA e l'innovazione sullo stato di attuazione del dettato normativo dell'art.50-bis 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.
Il DPCM 01.04.2008, inoltre, ha definito 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, unitamente alla presenza Centro di Gestione per i servizi di interoperabilità e cooperazione applicativa (CG-SICA), 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.

(C) Sicurezza della Rete: il Sistema Pubblico di Connettività
A partire dal 2006 è stato realizzato dal CNIPA per la pubblica amministrazione il network unico della PA per i servizi di connettività, mediante l'affidamento a quattro fornitori pre-qualificati (Q-ISP) dei servizi di trasporto IP necessari alla interoperabilità ed alla cooperazione applicativa della pubblica amministrazione italiana. Nodo centrale dell'architettura di SPC è la Qualified Exchange Network (QxN) che costituisce il punto di scambio del traffico dati in transito tra amministrazioni afferenti a Q-ISP differenti (traffico *infranet*).

L'architettura di SPC per l'interconnessione tra i quattro Q-ISP, permette di evitare le instabilità tipiche dei Neutral Access Point (NAP) Internet, grazie al governo diretto da parte di DigitPA delle interconnessioni tra i provider medesimi, che prevede:

- l'attribuzione e il confinamento delle responsabilità degli attori, attraverso il controllo diretto dell'infrastruttura di collegamento;
- garanzia di elevati livelli di qualità, sicurezza ed affidabilità al traffico *infranet*;
- ininfluenza delle politiche commerciali proprie degli operatori sulle modalità di *peering*;
- indipendenza dalle tecnologie, dalla qualità e dalle strategie di sviluppo implementate da ciascun operatore.

Data la centralità del ruolo di QXN, il Capitolato Tecnico della gara "multi-fornitore" ha stabilito elevati requisiti di qualità del servizio di interconnessione tra provider. L'infrastruttura tecnica necessaria a garantire questi elevati standard qualitativi comprende:

- architettura geograficamente distribuita attraverso due nodi: Roma (Namex) e Milano (MIX);
- disponibilità del servizio pari a 99,99%;
- ritardo di propagazione IP tra due nodi inferiore a 20 ms;
- probabilità di perdita di pacchetti IP inferiore allo 0,05%;
- NOC e SOC attivi 24 ore su 24 per 365 giorni l'anno;
- servizi centralizzati di DNS e NTP.

L'adozione di un'architettura completamente ridondata, anche geograficamente, è il risultato di una scelta condizionata dalla necessità di poter far fronte ad eventi potenzialmente in grado di causare l'indisponibilità dell'infrastruttura. Le politiche di instradamento (BGB), inoltre, implementate dai Q-ISP per i prefissi *infranet* assegnati alle PA di propria competenza, prevedono due modalità differenti di propagazione: verso QXN, quindi verso il nodo di interscambio del traffico tra i quattro fornitori, i prefissi infranet sono annunciati con una preferenza più alta, rispetto a quanto viene fatto per Internet. In questo modo, prediligendo il percorso più vantaggioso, le PA che utilizzano servizi di trasporto SPC attraverseranno sempre la rete QXN con i livelli di qualità e di sicurezza previsti; cittadini e imprese, da parte loro, non vedranno preclusa la fruizione dei servizi delle Amministrazioni, potendo sempre raggiungere i servizi delle PA attraverso la Internet.

Caratteristiche di resilienza dell'architettura SPC conseguono anche dalla possibilità di utilizzare la rete Internet come back-up del traffico infranet: in caso di guasto esteso a tutta la QXN, infatti, il traffico infra-amministrazione sarebbe veicolato attraverso il normale canale Internet, ancorché pregiudicando la qualità prevista per il trasporto dati ma non le funzionalità essenziali di interconnessione.
La gara a procedura ristretta "multi-fornitore" per la realizzazione della rete del SPC, nell'operare una selezione specifica tra i più grandi ed importanti[5] operatori di telecomunicazione presenti sul territorio italiano ha previsto la possibilità di una migrazione parziale delle Amministrazioni fornite da un Q-ISP nel caso di rescissione del contratto o di procedure fallimentari.

(D) Ruolo di DigitPA e del CERT-SPC
In questo contesto e coerentemente con gli obiettivi perseguiti con il rilascio delle presenti Linee Guida, DigitPA potrebbe assumere un ruolo di riferimento e di coordinamento delle iniziative in materia di protezione delle infrastrutture critiche nazionali per tutto ciò che riguarda la pubblica amministrazione nel suo complesso. A tal fine, l'Ente potrebbe essere investito di un ruolo di indirizzo, coordinamento ed assistenza per tutte quelle amministrazioni i cui sistemi ICT saranno identificati come infrastrutture critiche o risulteranno comunque interconnessi con quelli gestiti da soggetti privati ed identificati come ICN, anche al fine di accertarne la coerenza delle iniziative di protezione rispetto ai piani di CO/DR realizzati secondo le presenti Linee Guida.
Un'iniziativa che potrebbe competere a DigitPA è quella di realizzare un censimento dei sistemi IC interconnessi all'interno della PA ed attivare un tavolo di lavoro dove mettere a fattor comune i risultati di differenti progetti europei (es. MIA, MoTIA, Domino, NeISAS), al

5 le Pubbliche Amministrazioni sottoscrittrici dei Contratti Esecutivi SPC possono contare su una disponibilità del backbone dei provider almeno dell'ordine del 99,9999%. Questo tipo di parametro garantisce la disponibilità complessiva della rete della PA anche in caso di eventi disastrosi, sia dolosi che naturali.

fine di realizzare un progetto nazionale (MOSAICO) per la mappatura delle interdipendenze (logiche, fisiche, geografiche e cyber) in ambito pubblica amministrazione.

Il CERT-SPC[6], inoltre, potrà essere un centro di riferimento per la raccolta delle segnalazioni relative a minacce, vulnerabilità ed incidenti relativi ai sistemi ICT di quelle amministrazioni, provvedendo a veicolare le informazioni al CNAIPIC [7]previa definizione di una convenzione ai sensi del citato DM del 09.01.2008.
L'attività di analisi dei dati e delle comunicazioni ricevute dalle ULS delle amministrazioni, serviranno al CERT-SPC per definire periodicamente il quadro delle principali minacce informatiche che potrebbero interessare la PA nel suo insieme, consentendo – altresì – la definizione di un sistema di metriche condiviso per la classificazione del livello di rischio.
Per tali finalità, potrebbe essere demandato al CERT-SPC il compito di partecipare e/o coordinare lo svolgimento di esercitazioni che vedano coinvolte le PA insieme con altri operatori di ICN.
La realizzazione, infine, di un'efficace, tempestivo e codificato sistema di condivisione delle informazioni tra gli attori interessati rappresenta, infatti, il più importante fattore di successo delle politiche e delle iniziative di protezione delle infrastrutture e dei sistemi critici.

6 Il Computer Emergency Response Team del Sistema Pubblico di Connettività attivato dal 2008 presso DigitPA quale "referente centrale per la prevenzione, il monitoraggio, la gestione, la raccolta dati e l'analisi degli incidenti di sicurezza" (cit. DPCM 01.04.2008)
7 Il C.N.A.I.P.I.C. è l'articolazione della Polizia delle Telecomunicazioni incaricata in via esclusiva della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

9 CONCLUSIONI

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 capitolo 1 e nel paragrafo 2.5. sono più diffusamente trattate nelle 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 a DigitPA 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 ala Ministro della Pubblica Amministrazione e innovazione, sarà possibile perseguire l'obiettivo di assicurare l'omogeneità delle soluzioni di continuità operativa.
E' affidato poi al Ministro per la pubblica Amministrazione e l'innovazione il compito di informare al riguardo, con cadenza annuale, il Parlamento.

Compito di DigitPA 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: LA BUSINESS IMPACT ANALYSIS (BIA)

Il termine “metodologia” indica un insieme strutturato di attività che, condotte in un dato ordine, definiscono un percorso che porta a un obiettivo prefissato. In questa appendice verranno sinteticamente richiamati i passi di un possibile percorso attraverso il quale una pubblica amministrazione può studiare, progettare e realizzare una soluzione di continuità operativa adeguata alle proprie esigenze.
Non tutti i passi metodologici descritti nel seguito sono indispensabili per progettare e realizzare correttamente una soluzione di continuità. A seconda delle caratteristiche e del contesto della singola amministrazione, alcuni passi potrebbero essere superflui, o da condurre solo per grandi linee, in quanto l’impegno richiesto per la loro esecuzione potrebbe non essere giustificato dai benefici ottenibili.
In ogni caso, una conoscenza del percorso completo può essere utile per identificare quali passi – nei vari casi – siano indispensabili e quali invece possano essere tralasciati. L’obiettivo finale da raggiungersi attraverso passi intermedi che possono essere diversi a seconda del percorso intrapreso, è generalmente una soluzione tecnico-organizzativa in grado di soddisfare le esigenze di continuità esistenti.
Alcune metodologie, in realtà, giungono soltanto fino alla determinazione della soluzione migliore (o, meglio, più adeguata alle esigenze) ed alla stima di impegno economico per la realizzazione della soluzione stessa. In questo documento, viceversa, faremo rientrare nel percorso metodologico anche la fase di realizzazione, di gestione e di manutenzione della soluzione.
Anche la metodologia proposta nel proseguo è soggetta ad una ciclicità ispirata al ciclo di Deming (Plan, Do, Check, Act) prevedendo, dopo la fase iniziale di studio/analisi del contesto, il disegno della soluzione tecnologico-organizzativa che meglio risponde alle esigenze di continuità richieste, la realizzazione e il mantenimento della soluzione.

Tutti i percorsi metodologici esistenti nella letteratura tecnica hanno come punto di partenza lo studio del contesto di riferimento, cioè del quadro tecnologico e organizzativo all’interno del quale esiste un’esigenza di continuità operativa da soddisfare. In generale, lo studio del contesto è indirizzato a stabilire la tipologia di eventi dalla quale l’amministrazione intende proteggersi: una corretta identificazione degli eventi d’interesse permette di restringere in anticipo la scelta tra le soluzioni utili per eliminare o mitigare gli effetti degli eventi stessi.

Per le finalità di CO e DR, nel seguito sarà posta particolare attenzione agli eventi che interrompono l’erogazione dei servizi di pertinenza dell’amministrazione a causa dell’indisponibilità prolungata del sistema informatico.
Le soluzioni di continuità, infatti, prendono in considerazione l’impatto di un evento e non le sue cause, la relazione tra l’impatto e la causa, origine dell’indisponibilità, concordemente con quanto sancito dagli standard ISO27001 e BS25999, è determinata attraverso il legame tra la BIA ed il processo di Analisi dei Rischi (RA). La RA ha l’obiettivo di identificare quali siano gli scenari di rischio che insistono sul patrimonio informativo, a supporto dell’erogazione dei processi dell’Amministrazione, attraverso i quali si qualificano gli eventi / minacce che presentano maggior probabilità di concretizzarsi (e.g. in funzione dei livelli di vulnerabilità, delle contromisure in essere, dell’appetibilità dei servizi offerti), generando un danno per l’Amministrazione. Si individuando pertanto le possibili cause di indisponibilità quali ad esempio diffusione di virus, interruzione dell’alimentazione elettrica, incendio alla sala CED, etc..).
Obiettivo della RA è determinare il valore di rischio, rispetto al patrimonio informativo che supporta i processi critici dell’Amministrazione, sulla base del rapporto tra la probabilità di accadimento di un evento (o minaccia), il grado di esposizione (vulnerabilità) ed in funzione dell’impatto determinato nella fase di Business Impact Analisys (nel seguito BIA). La RA ha pertanto lo scopo di declinare gli scenari di rischio che potrebbero, se concretizzatesi, produrre danni rilevanti all’Amministrazione anche secondo quanto stimato nella BIA. Per scenari di rischio si intende la definizione di quali siano gli eventi (volontari o involontari, endogeni o esogeni, logico / fisici o di tipologia organizzativa, ecc...) che per una determinata risorsa (di cui si è stimato il danno originato da un suo guasto) sono critici.

La BIA, infatti, (Business Impact Analysis, termine inglese traducibile con "valutazione dell'impatto sull'operatività") è la metodologia da utilizzare al fine di determinare le conseguenze derivanti dal verificarsi di un evento critico e di valutare l'impatto di tale evento sull'operatività dell'amministrazione.

La Business Impact Analysis, infatti, ha l'obiettivo di correlare specifiche componenti di sistema con i servizi critici che forniscono e, sulla base di tali informazioni, caratterizzare le conseguenze di una indisponibilità delle componenti stesse.[8] Quindi, la BIA prevede due macrofasi: il censimento dei processi fondamentali[9] (*mission critical*) e la loro correlazione ai sistemi ICT.

Normalmente, la BIA valuta l'impatto di un evento sull'operatività su base economica, valutando cioè la perdita economica causata dal verificarsi di un evento. Questo approccio, tuttavia, non è immediatamente applicabile al contesto della Pubblica Amministrazione. Nel settore pubblico, difatti, l'interruzione dei servizi erogati comporta danni non immediatamente "monetizzabili": le perdite (e dunque l'impatto) devono essere valutate tenendo conto dell'insieme dei seguenti aspetti:

- aspetti economici (mancata o ritardata riscossione di tributi, esborso di oneri aggiuntivi conseguenti il mancato pagamento a cittadini o imprese, ecc.);
- aspetti sociali (la non disponibilità di servizi sociali critici può generare problemi di ordine pubblico);
- aspetti reputazionali (perdita di credibilità da parte delle istituzioni);
- aspetti normativi (mancata o differita attuazione di norme di legge).

Mediante specifiche valutazioni da parte dell'Amministrazione, le attività di BIA consistono in:

– Identificazione dei processi chiave considerati nel perimetro di analisi (aspetti da valutare ai fini della soluzione di **continuità dell'Amministrazione**);
– Delineare la criticità di ciascun processo (**Classificazione dei processi** in funzione degli impatti)
– Determinare la criticità delle risorse che contribuiscono all'erogazione dei processi (**Classificazione delle risorse**) e le loro interdipendenze;
– **Individuare i tempi di indisponibilità massima sostenibili** per ciascun processo definita in termini di RTO ed RPO.

Al termine dei passi descritti, in genere viene prodotto un documento finale di BIA: l'indice del documento prodotto al termine della BIA può essere strutturato seguendo lo schema di seguito riportato che traccia le singole fasi di una metodologia di BIA

Aspetti da valutare ai fini della soluzione di continuità dell'Amministrazione

Rispetto ai Servizi considerati come prioritari ed agli Obiettivi dell'Amministrazione definiti nella Politica di Continuità Operativa, è importante procedere all'identificazione puntuale dei processi legati all'erogazione dei Servizi e delle caratteristiche di cui si ritiene opportuno tenere conto durante le analisi dal punto di vista della continuità operativa.
Per ciascun processo possono essere oggetto di valutazione parametri quali:

[8] Libera traduzione dal NIST "Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34, p. 16)

[9] Un servizio ICT, in questo ambito, è inteso come il prodotto di un processo: può accadere, pertanto, che tale processo sia correlato ad altri processi (anche non ICT) che, indirettamente, concorrono all'erogazione del servizio ICT. Se è vero che per il percorso di autovalutazione proposto ci si è concentrati sui servizi ICT, non può non tenersi presente che il processo rappresenta il punto dove concentrare l'attenzione per garantire la CO di un organizzazione globalmente intesa, al fine di evitare che la mancata CO di processi correlati al processo che eroga il servizio possa inibire la CO del servizio stesso.

1. il Fattore di blocco, che esprime se il processo in questione è bloccante o meno per il Servizio a cui si riferisce; ·
2. le Relazioni con altri processi: flussi di informazioni (qualificando se sono bloccanti o non bloccanti), SLA/KPI;
3. gli Attori coinvolti;
4. le Statistiche di indisponibilità nel tempo (ove disponibili);
5. i vincoli sui periodi di operatività che indicano se esiste uno specifico lasso temporale nel quale il processo deve assolutamente essere disponibile (e.g. applicazioni che computano e gestiscono le buste paghe dei dipendenti);
6. i vincoli normativi e/o contrattuali; il grado di complessità di un processo durante il suo ciclo di vita; la frequenza, che nei processi periodici ne qualifica la frequenza di esecuzione (e.g. una volta al mese, alla settimana);
7. il supporto all'esecuzione (Manuale / Automatico) che esprime il livello di automazione del processo.

Classificazione dei processi

Partendo dagli aspetti precedentemente richiamati, vengono individuati i processi direttamente legati all'erogazione del servizio e quelli di supporto e, di ciascuno, l'Amministrazione valuta la criticità in termini di importanza del processo rispetto ai diversi parametri di riferimento definiti.
Una lista esemplificativa di processi da includere nelle attività in oggetto può essere:

1. Relazioni esterne ed istituzionali;
2. Risorse Umane e Relazioni Sindacali;
3. Amministrazione;
4. Pianificazione Finanziaria & Controllo;
5. Sistemi informativi;
6. Servizi ad altre amministrazioni;
7. Servizi alle imprese;
8. Servizi al cittadino.

Un approccio efficace per dimensionare la criticità, nel mondo della Pubblica Amministrazione, può esprimersi attraverso l'identificazione di coefficienti qualitativi che esprimano la classificazione dei processi analizzati.
Per Classificazione dei Processi si intende una loro valutazione, basata su diversi parametri che vanno dall'importanza e ruolo, ad esempio perché direttamente legati all'erogazione di servizi essenziali al cittadino, al livello di complessità e che consente di stilare un scala di priorità di rilevanza e dunque di ripristino.
A titolo esemplificativo sono riportati alcuni indici per il calcolo della Criticità dei processi:

Indice di rilevanza (IR)

Si tratta di individuare un Valore Qualitativo di Rilevanza per il processo in relazione, ad esempio, al fatto che il processo sia legato direttamente all'erogazione di un servizio, oppure che vi concorra in maniera indiretta, oppure sia un processo legato alla gestione efficiente ed economica dell'Amministrazione, ecc..

Di seguito una possibile matrice di riferimento per l'individuazione della criticità di un processo per l'organizzazione.

Tipologia	Descrizione	Valore Qualitativo Di Rilevanza
Processi di erogazione dei Servizi	Processi attraverso cui l'Amministrazione eroga un servizio in maniera diretta agli utenti	4
Processi di Supporto all'erogazione dei Servizi	Processi che, pur non consentendo direttamente l'erogazione di un Servizio, vi concorrono comunque in maniera determinante	3
Processi di Gestione	Processi che concorrono in maniera determinante alla gestione efficiente ed economica dell'Amministrazione	2
Processi di Controllo	Processi non direttamente legati all'erogazione di un Servizio ad utenti interni o esterni ma finalizzati ad esercitare il controllo della gestione per il rispetto dei risultati previsti	1

Tabella 1 - criticità di un processo

Indice di complessità

La valutazione dell'indice di complessità di un processo può essere effettuato sulla base di almeno due parametri principali:

- Il Livello di Interdipendenza (LI) ovvero il livello di correlazione del processo in esame con altri processi;
- il Livello di Complessità (LC), ovvero il livello di articolazione del processo che può richiedere diverse fasi di elaborazione, competenze altamente specialistiche, un elevato numero di risorse per la sua esecuzione. Un metodo di aggregazione è rappresentato nella tabella seguente:

Livello di Interdipendenza (LI)	Indice di Complessità (IC)= LI*LC		
Correlato a più di 3 processi	1*3=3	2*3=6	3*3=9
Correlato a meno di 3 processi	1*2=2	2*2=4	3*2=6
Singolo	1*1=1	2*1=2	3*1=3
Livello di Complessità (LC)	Grado di Complessità Basso	Grado di Complessità Medio	Grado di Complessità Alto

Tabella 2 - Indice di complessità

Indice di sensibilità

La valutazione della Sensibilità del processo (SP) considera quali possibili caratteristiche del processo da valutare, la Tipologia di utenti cui i Servizi dell'Amministrazione sono rivolti e i possibili Impatti in termini di reputazione in caso di indisponibilità dei servizi stessi. Per quanto riguarda la Tipologia di utente (UT), fruitore del servizio, si possono considerare ad esempio, le seguenti categorie, in ordine crescente di importanza:

- utente interno;
- utente esterno generico;
- servizio rivolto alle Autorità o Pubbliche Amministrazioni Nazionali ed Internazionali;
- servizio rivolto alla collettività.

Per quanto riguarda la Perdita di Reputazione (PR), questa può essere espressa attraverso scenari quali:

- Affidabilità (A) – L'indisponibilità del processo può ingenerare nell'utente del servizio la sensazione che l'Amministrazione non sia in grado o non tiene cura della qualità dei servizi offerti;
- Responsabilità sociale (R), che vuole rappresentare se l'Amministrazione applica le normative che ne disciplinano l'operato
- Politica di innovazione (P), che mostra se l'Amministrazione è o meno capace di assicurare la qualità del servizio offerto anche mediante l'utilizzo esteso delle nuove tecnologie.

L'Indice di Sensibilità del processo può essere calcolato moltiplicando il valore corrispondente al UT per il numero di scenari di impatto coinvolti:

$$SP = f_1(UT, A, R, P, G)$$

e dove la funzione di aggregazione è rappresentabile come segue:

$$f_1 = \left(\sum UT * parametri\ (A, R, P)\right)$$

Le variabili A, R e P sono variabili binarie [0, 1] che esprimono la presenza o meno della perdita di reputazione corrispondente.

Frequenza del processo e Livello di automazione e (Fr e LA)

Due parametri che consentono di qualificare l'operatività di un processo sono il livello di automazione, che mostra il grado di automazione previsto per il processo che, pertanto, è dipendente dalla continuità delle risorse ICT su cui si poggia e la frequenza di esecuzione, che esprime il grado di disponibilità del processo nel tempo.

- Frequenza (Fr): che esprime la periodicità di esecuzione del processo;
- Livello di automazione (LA): che considera l'automazione del processo da manuale, semi-manuale , semi-automatico e automatico.

Classificazione delle risorse

Nella presente fase, per ogni processo censito, si identificano quali siano le risorse che ne supportano o si relazionano alla sua erogazione, e, laddove applicabile, all'erogazione di altri processi. Le tipologie di risorse che possono essere considerate a supporto dell'erogazione dei processi sono ad esempio, risorse ICT quali applicazioni, hardware, mezzi di comunicazione, oppure dati e informazioni, risorse umane, supporti cartacei, ecc..Anche in questo caso le valutazioni effettuate dall'Amministrazione consentono di determinare una Classificazione, questa volta delle risorse. Questa fase permette, infatti, di definire una classifica dimensionando per ciascuna un coefficiente di peso (PR) rappresentativo:

- delle peculiarità della risorsa;
- del suo grado di importanza / rilevanza / interazione con il processo;
- del carattere della risorsa bloccante o meno per l'erogazione del processo.

Il coefficiente di peso della risorsa sintetizza parametri:

1. di natura intrinseca, caratteristici della risorsa;
2. funzionali ai processi che la risorsa stessa supporta.

La seguente figura propone alcuni esempi di parametri da contemplare e valorizzare per delineare il peso delle risorse:

Parametri	Scala	Informazione	Applicazione	...	Ecc ...
Varianza del dato (utile anche per indirizzare opportunamente l'RPO)	1 (> 3gg) 3 (1-3 gg) 5 (<1gg)	x			
Classificazione del dato	pubblica (1) interna (2) confidenziale (3) Secret (4)	x	x		
Cogenza applicabile	Non cogente (0) Cogente (5)	x	x		
Grado di esposizione all'impatto di immagine e/o legale	Nullo o trascurabile (0) Basso(1) Alto (3) Critico(5)	x	x		
Perdita economica	Parametro che stima se la perdita di disponibilità della risorsa induce perdite dirette finanziarie - Nulle (0) - Assorbili (1) - Gravi (2) - Compromissive (3)		x		
Livelli di servizio attesi	SLA continuità assoluta – 5 SLA (>97%) - 3 SLA (90 - 97%) – 2 SLA (<90%) - 1		x		
	...				
Peso risorsa	FORMULE di Aggregazione	F(parA, parB, ..., parM)	F (par1, par2, ..., parn)	...	...

Le formule di aggregazione dei parametri, necessari a calcolare i pesi da attribuire alle risorse, vanno scelte tenendo in conto dell'enfasi che si vuole dare a un parametro rispetto agli altri, per il calcolo finale.

Per la classificazione delle risorse può essere utile includere anche il parametro rappresentato dal **coefficiente di contribuzione** della risorsa all'erogazione del processo. Il parametro in questione sintetizza il livello di correlazione e di importanza di impiego della risorsa per lo specifico processo e considera ad esempio se la risorsa è marginalmente correlata al processo, se esiste una correlazione ma non è determinate, o se la risorsa è determinate per l'erogazione del processo.

Il **Coefficiente di Contribuzione CC** della risorsa che esprime, in rapporto alla continuità del processo che la risorsa supporta, se quest'ultima sia ininfluente, utile, importante, essenziale (bloccante).

CC	100%: bloccante
	75%: influente ma non bloccante
	25%: parzialmente influente
	12,5%: non influente
	0%: non pertinente

Tabella 1 - coefficiente di blocco

Sulla base dei parametri di cui l'Amministrazione ritiene opportuna la valutazione, alla risorsa generica è associata una coppia di coefficienti, il Peso della Risorsa (PR) e Coefficiente di Contribuzione (CC).

Sintesi dei Risultati

Censiti i processi, eventualmente suddivisi in sotto processi (o MCA – Attività critica), e definiti i coefficienti di peso delle risorse interessate da ciascuno, è opportuno costruire una tabella di correlazione processi - risorse per:

- Collegare il processo o MCA alle rispettive risorse;
- Individuare tutte le risorse che supportano più di un processo e che pertanto risultano avere una criticità, a parità di importanza dei processi, maggiore;
- Computare opportunamente gli impatti prodotti dall'indisponibilità di un processo in rapporto alla criticità di ciascuna delle risorse che lo supportano: **Valore di Impatto di ciascun Processo,** che

permette di classificare i processi dal più critico al meno critico dal punto di vista delle esigenze di continuità operativa;
- Calcolare gli impatti sulle risorse partendo dal valore di impatto dei processi e dal numero di processi che condividono la stessa risorsa**: Livello di Criticità delle risorse,** che consente di comprendere l'importanza di ciascuna tipologia di risorsa e quindi la relativa priorità di ripristino.

Pertanto, censiti i processi, calcolato il Valore di Classificazione (VC) di ciascun processo e definiti i coefficienti di peso e di contribuzione delle risorse interessate da ciascuno, è possibile:

- **collegare** il processo alle rispettive risorse, attraverso il coefficiente di contribuzione;
- **individuare** tutte le risorse che supportano più di un processo;
- **calcolare** gli impatti sulle risorse partendo dal valore di impatto dei processi e dal numero di processi che condividono la stessa risorsa, ciascuno con il proprio coefficiente di contribuzione.

RTO e RPO

Il calcolo dei valori di RTO e RPO ha come obiettivo, come visto nei precedenti capitoli, di individuare le tempistiche entro cui il ripristino deve avvenire. Nello specifico l'indice RTO esprime l'arco temporale massimo entro cui il ripristino delle risorse minime deve essere garantito, al fine di contenere gli impatti, legati all'indisponibilità, a livelli sopportabili per l'Amministrazione, mentre l'RPO rappresenta l'intervallo temporale massimo a cui far riferimento per individuare il punto di ripristino dei dati e/o del sistema.
Per dimensionare l'RTO si deve computare l'impatto (sia questo valutato anche qualitativamente) in funzione del tempo, ipotizzando per lo scenario di impatto una curva rappresentativa (lineare, esponenziale, asintotica, ecc. o una aggregazione di quelle indicate) che influenzi i valori dei processi, del peso e del coefficiente di contribuzione delle risorse, affinché questi assumano rilevanze differenti al crescere dei tempi di indisponibilità. L'RTO si esprime quando la curva degli impatti comincia a divergere a valori non più accettabili dall'Amministrazione.
L'RPO si esprime tenendo in considerazione il grado di varianza dei dati e delle configurazioni dei sistemi /piattaforme, la possibilità ed il tempo necessario per ricostruire la situazione precedente al disastro dal punto di ripristino (dall' ultimo salvataggio delle informazioni disponibili).
Ad esempio, alcuni criteri di calcolo per RTO potrebbero essere la divergenza della curva degli impatti, oppure la stima dei tempi di ripristino, mentre per RPO potrebbero essere rappresentati dalla varianza dei dati o dalla capacità di ricostruire le modifiche intercorse tra il disastro ed ultimo back up (punto di ripristino).
Il dimensionamento di questi due parametri definisce delle Classi di ripristino in cui i servizi ricadono, caratterizzando notevolmente le strategie e le soluzioni di CO.

RISK ASSESSMENT

Al fine di completare il processo di analisi complessiva, utile alla redazione dello studio di fattibilità della CO, congiuntamente alla BIA, occorre effettuare un Risk Assessment (RA), ovvero l' analisi per determinare il valore dei rischi di accadimento di un evento che possa interrompere la continuità operativa. Obiettivo della fase è determinare, sul patrimonio informativo che supporta i processi critici dell'Amministrazione, il **valore di rischio** in rapporto alla probabilità di accadimento di un evento (o minaccia), al suo grado di esposizione (vulnerabilità) ed in funzione dell'impatto determinato nella fase di BIA. Il processo in questione ha, pertanto, lo scopo di declinare gli scenari di rischio che potrebbero, se concretizzati, produrre danni rilevanti all'Amministrazione secondo quanto stimato nella BIA. Per scenari di rischio si intende la definizione di quali siano gli eventi (volontari o involontari, endogeni o esogeni, logico / fisici o di tipologia organizzativa, ecc…) che, per una determinata risorsa (di cui si è stimato il danno originato da un suo guasto), sono critici.
Il primo passo del processo di analisi di rischi riguarda l'individuazione delle diverse tipologie di risorse che supportano un determinato processo dell'Amministrazione.
Per ciascuna delle risorse vengono valutate le minacce, ovvero gli eventi la cui manifestazione può determinare un danno per un sistema o per le informazioni trattate da quest'ultimo. Tale danno deriva dalla compromissione di uno o più degli attributi di riservatezza, integrità e disponibilità. Ovviamente, una minaccia può non rappresentare un rischio se l'asset in questione non presenta vulnerabilità, sfruttabili dalla minaccia stessa. Pertanto, per determinare la probabilità di accadimento di una minaccia, si devono

analizzare anche le vulnerabilità che favoriscono la sua realizzazione e contestualmente le contromisure che sono impiegate per contrastarla.
La valutazione del valore della Minaccia relativo ad uno specifico asset può ritenersi accurata quando ad informazioni di tipo oggettivo, quali ad esempio i dati statistici rappresentativi della frequenza con cui in passato questa si è concretizzata, si uniscono anche valutazioni inerenti le caratteristiche distintive della minaccia: in caso di minacce dal carattere intenzionale, ad esempio valutazioni sul grado di competenza tecnica necessario per attuare un determinato evento, mediata altresì con valutazioni sull'appetibilità che potrebbe indurre un agente ostile a mettere in atto la minaccia, potrebbero, insieme alla frequenza storica, rappresentare compiutamente l'attuabilità e la probabilità di accadimento della minaccia.
Ai fini della valutazione dei rischi è importante confrontare le varie minacce con le diverse possibilità di relativa compromissione degli attributi di sicurezza così come dalla loro inter-correlazione relativamente diverse risorse in esame. Le seguenti figure ne mostrano una possibile rappresentazione:

CRITERI DI VALUTAZIONE DELLA MINACCIA				LIVELLO DI ESPOSIZIONE
Sorgente			Frequenza	
Capacità	*Intento*	*Valutazione*		
Si	Sì	altamente attiva	Bassa	MEDIO
			Media	ALTO
			Alta	
Si	No	mediamente attiva	Bassa	BASSO
			Media	MEDIO
No	Si		Alta	ALTO
No	No	scarsamente attiva	Bassa	BASSO
			Media	
			Alta	MEDIO

Figura 1 – criteri valutazione minaccia

Risorse / Minacce	Accesso non autorizzato	**Compromissione delle informazioni**	Utilizzo improprio	**Diffusione di malicious software**	Errori di manutenzione	**Mancanza organizzativa**	Assenza di personale chiave	**Danneggiamento di asset**	Furto	**Incidenti infrastrutturali**	Malfunzionamento	**Evento di forza maggiore**	Violazione della legge o di altri regolamenti
Infrastruttura Fisica	RI		RI		ID	RD				ID		ID	RID
Sistemi Ausiliari	I				ID	D	D	ID		D	D	D	
Rete Dati	RI	RID	D	ID	ID	D	D	ID			D		RID
Apparati ICT	RI		ID		ID	D	D	ID	D		ID		RID
Sistema Operativo	RI	RI	RI	RID	ID	D	D		D		D		RID
DataBase	RI	RI	RI	RID	ID	D	D		D		D		RID
Software applicativo	RI	RI	RI	RID	ID	D	D		D		D		RID
Servizi Web	RI	RI	RI	RID	ID	D	D		D		D		RID
Organizzazione (processi, procedure, policy)						RID							RID
Personale						RD	D						

Figura 2 – matrice relazione risorse - minacce

L'analisi delle minacce è, perciò, utile a determinare il **Livello di Vulnerabilità** di un asset per una specifica minaccia, il cui calcolo deve considerare:

a) la capacità della vulnerabilità, se sfruttata, di ledere la riservatezza (R), integrità (I) e/o disponibilità (D) dell'asset, producendo danni e fermi della risorsa,
b) la frequenza con cui in passato una minaccia ha sfruttato la vulnerabilità in oggetto,
c) il grado adeguatezza e di completezza delle contromisure implementate.

Combinando i due parametri (minaccia e vulnerabilità) si perviene al dimensionamento del **livello di esposizione** di una risorsa che indica la probabilità di successo associata ad un attacco, portato da una minaccia sfruttando una specifica vulnerabilità.
Associando questo parametro con la **criticità dell'asset, calcolato nella fase di BIA,** si determina il livello di rischio specifico relativo alle varie Risorse che si configura come una funzione che ha come parametri

$$\text{MoR} = f_{\Sigma}(I, M, V),$$

dove I = impatto
M = Minaccia
V = Vulnerabilità
MoR = misura del Rischio

Profilo di Rischio

Il profilo di rischio rappresenta uno strumento decisionale per la definizione delle strategie di Continuità Operativa. E' rappresentativo della coppia di informazioni **(rischio, impatto)** associati ad una risorsa. Stabiliti pertanto:

1) gli impatti associati ai processi / risorse, e gli obiettivi di Continuità Operativa (RPO,RTO);
2) i valori di rischio,

si hanno le informazioni necessarie per rappresentare "Causa" ed "Effetto". Per ciascun processo infatti è possibile determinare l'impatto per l'Amministrazione legato ad una indisponibilità del processo stesso ed il rischio che questo accada in rapporto a specifiche inadeguatezze dell'infrastruttura di sicurezza, piuttosto che di assenza di opportune misure di protezione per la continuità operativa del business. In altre parole, conoscendo il livello di classificazione dei processi (dalla BIA), gli scenari a più alto rischio di indisponibilità delle risorse critiche che erogano i suddetti processi (dall'RA), si possono individuare:

a) Le minacce che possono inficiare la disponibilità di risorse critiche, ad alto impatto per l'Amministrazione;
b) Diagrammi, nei quali sono illustrate le relazioni esistenti tra i valori di rischio che insistono su ciascun asset e gli impatti derivanti.

APPENDICE B: ULTERIORI ASPETTI IN TEMA DI ORGANIZZAZIONE DELLE STRUTTURE DI GESTIONE DELLA CONTINUITÀ OPERATIVA

Le Amministrazioni particolarmente complesse potranno individuare oltre al Comitato di gestione della crisi e al Gruppo di supporto di cui si è trattato nel capitolo 4 anche ulteriori strutture organizzative e i gruppi di seguito indicati, nonché tener conto dei suggerimenti di seguito riportati.

Il Gruppo di Coordinamento Tecnico ed ulteriori possibili gruppi

E' possibile individuare il Gruppo di coordinamento tecnico quale responsabile delle attività operative e tecniche connesse con l'esecuzione delle procedure di recupero e rientro. Nel dettaglio, in condizioni ordinarie tali attività sono:

- esercitazioni e test periodici;
- manutenzione dell'infrastruttura tecnologica e applicativa di recupero.

Mentre in condizioni di emergenza le attività sono:

- coordinamento del personale operativo in emergenza;
- organizzazione dei trasporti e della logistica del personale operativo in emergenza;
- notifica dello stato di avanzamento al Comitato di gestione della crisi;
- gestione del budget per spese straordinarie legate all'emergenza;
- monitoraggio del funzionamento delle applicazioni e dei sistemi in configurazione di ripristino;
- controllo e verifica dell'esito delle procedure di salvataggio e quadratura;
- interfaccia con gli outsourcer in condizioni di crisi.

È opportuno individuare formalmente i componenti di questo Gruppo, che possono essere:

- il responsabile dei sistemi informativi dell'amministrazione, che lo presiede;
- i responsabili delle unità organizzative tecniche, applicative e logistiche.

Il Gruppo di coordinamento tecnico potrebbe anche aver necessità di organizzare altri gruppi di persone a proprio supporto (tecnico, decisionale e organizzativo) che agiscano alle sue dipendenze per tutto il periodo d'emergenza. Ad esempio, potrebbe esserci la necessità di formare:

- un gruppo applicativo;
- un gruppo operativo;
- un gruppo di rientro.

Il gruppo applicativo è responsabile di tutte le attività sulle applicazioni e i dati ad esse associati. In particolare, a questo gruppo può essere assegnato, in condizioni di emergenza, il compito di:

- monitorare il funzionamento delle applicazioni e attivare eventuali interventi correttivi;
- sincronizzare le proprie attività con quelle del gruppo operativo.
- controllare l'esito delle procedure di salvataggio;
- assicurare il funzionamento dell'infrastruttura applicativa nel sito alternativo.

Il gruppo operativo è responsabile di tutte le operazioni che coinvolgono i sistemi informatici e la rete di telecomunicazioni. In particolare, a questo gruppo può essere assegnato, in condizioni di emergenza, il compito di:

- monitorare il funzionamento dei sistemi;
- coordinare le attività con quelle del gruppo applicativo.

Il gruppo di rientro è responsabile di tutte le operazioni necessarie a garantire la ripresa della normale operatività presso il sito di esercizio. Per la natura delle attività da supportare e per l'estrema variabilità delle emergenze (e l'ampio numero degli scenari d'emergenza possibili), il compito del gruppo di rientro è da considerarsi molto gravoso.
In particolare, a questo gruppo può essere assegnato, in condizioni di emergenza, il compito di:

- rilevare i danni (la valutazione dei danni deve essere presentata al più presto al Comitato, e deve essere aggiornata frequentemente);
- gestire tutte le operazioni di rientro;
- testare l'infrastruttura ripristinata nel sito di esercizio.

La comunicazione tra i diversi gruppi di lavoro descritti deve essere basata sul principio che chi è incaricato di eseguire una procedura:

- comunica alla persona o alla struttura superiore, a richiesta, lo stato in cui si trova;
- riceve notizia di tutte le decisioni che lo riguardano e dei riflessi di queste sulle procedure nelle quali è coinvolto.

I processi di formazione, informazione e sensibilizzazione

Può essere utile attuare processi di formazione, informazione e sensibilizzazione, da effettuare con una logica top-down sono da sponsorizzare da parte dei massimi vertici dell'amministrazione, in quanto fattori importanti almeno quanto quelli tecnologici. Principali argomenti da trattare nell'ambito della formazione del personale addetto alle operazioni di mantenimento della continuità sono i seguenti:

- definizione di emergenza e di disastro;
- struttura organizzativa per l'emergenza;
- priorità decisionali e gestione dei rapporti interpersonali durante l'emergenza;
- canali di comunicazione e riferimenti informativi alternativi;
- procedure specifiche per settore;
- processo di rientro.

Per quanto riguarda gli utenti, il piano di formazione dovrà indirizzarne i comportamenti in caso di emergenza e l'uso di specifici strumenti quali i canali d'informazione d'emergenza e le procedure alternative per i servizi.

Per quanto attiene al processo di informazione e sensibilizzazione diffusa di tutto il personale, è da tener presente che la buona riuscita del Piano dipende da un gran numero di componenti dell'organizzazione.

Obiettivi essenziali del piano formativo possono essere:

- concetti di disastro;
- organizzazione, ruoli e limiti di azione durante le emergenze;
- linee guida di comportamento.

I contenuti della sensibilizzazione possono comprendere i seguenti temi:

- processi di comunicazione in situazione di emergenza;

- utilizzo di strategie di comunicazione alternative;
- procedure di ripristino.

Si sottolinea anche l'importanza delle sessioni di simulazione, specialmente di quelle (concettuali) destinate ai vertici dell'amministrazione, in particolare al Comitato di gestione della crisi, il quale dovrà sottoporsi a sedute periodiche in cui verificare e affinare la capacità di valutare gli imprevisti e di reagire alle situazioni di emergenza.

APPENDICE C: STRUMENTO DI SUPPORTO PER L'AUTOVALUTAZIONE

In questa parte viene illustrato il modello matematico messo a punto per realizzare la funzione di autovalutazione secondo i criteri generali descritti nei precedenti paragrafi.

Generalità

Il modello matematico si basa sulla rilevazione di alcuni specifici parametri, opportunamente scelti, i quali descrivono gli aspetti significativi di criticità e/o complessità dell'Amministrazione lungo le tre direttrici del servizio, dell'organizzazione e della tecnologia.

Ciascun parametro viene valutato mediante una scala quali-quantitativa costituita da una lista di scelte predeterminate, che rispecchiano le possibili alternative associate al parametro stesso. A ciascuna scelta alternativa è internamente associato un opportuno valore numerico che ne quantifica convenzionalmente la rilevanza relativamente alle altre scelte possibili per il medesimo parametro.

Ciascun parametro è inoltre caratterizzato da un *peso* che ne quantifica la rilevanza con riferimento agli altri parametri della medesima direttrice.

Per ciascuna direttrice i parametri concorrono quindi a formare un *indice di criticità* il quale viene calcolato come *combinazione lineare* dei valori di ciascun parametro secondo il proprio peso, successivamente normalizzata su un opportuno intervallo.

In pratica, detto p_i il peso del parametro i-esimo, e v_i lo specifico valore selezionato per esso, l'indice è calcolato mediante la seguente formula:

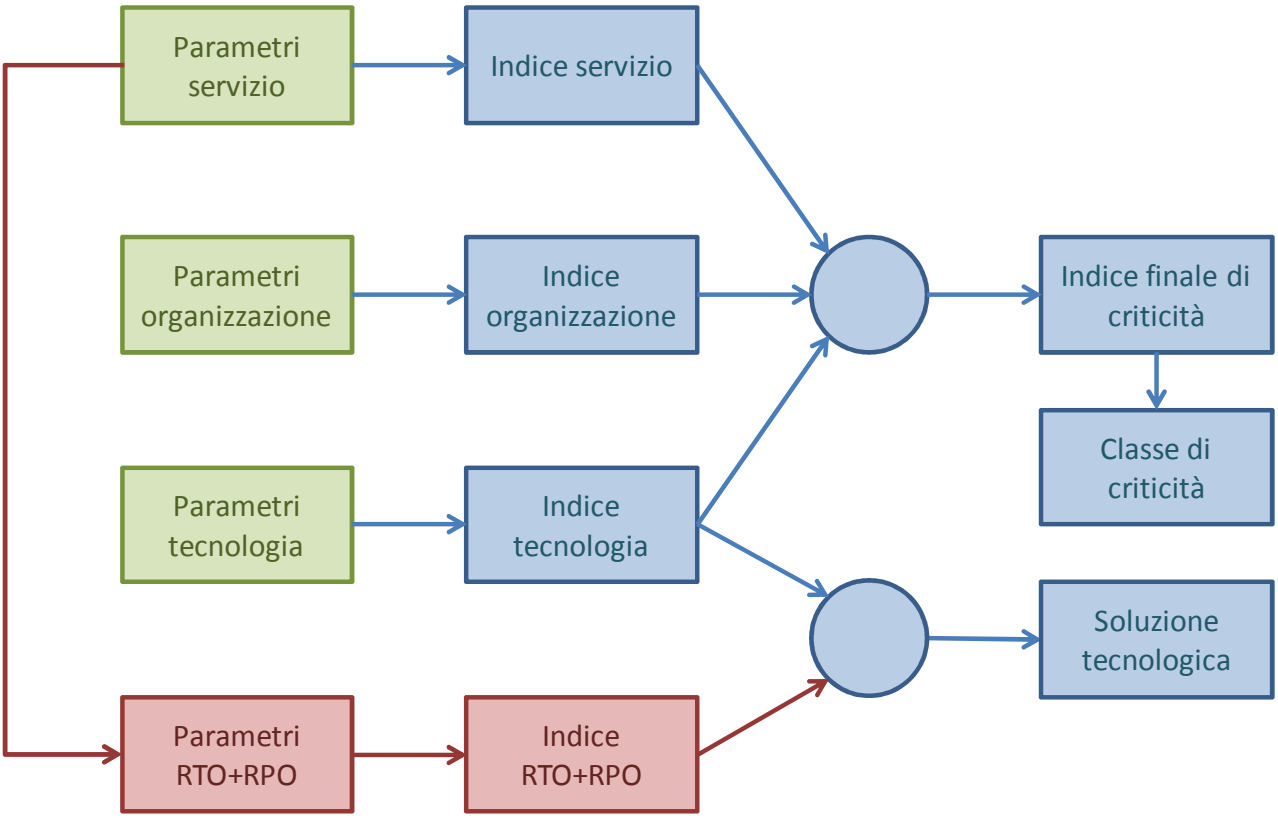
$$I = \frac{\sum_i p_i v_i}{\sum_i p_i}$$

Il valore dell'indice è normalizzato. I tre indici finali ottenuti dalla valutazione, uno per ciascuna direttrice, concorrono quindi a determinare l'indice complessivo di criticità del servizio in analisi. Il suo valore consente inoltre di associare al servizio in esame una delle possibili classi di criticità della soluzione di DR.

L'identificazione della più opportuna soluzione tecnologica (anche detta *Tier*) non è tuttavia direttamente associata alla classe di criticità risultante ma avviene applicando un'ulteriore formula la quale prende in considerazione due distinti indicatori: il primo è rappresentato da un indice che rappresenta i valori di RTO+RPO desunti da alcuni dei parametri indicati nella direttrice del servizio, ed il secondo è costituito dall'indice precedentemente calcolato per la direttrice della tecnologia; tali due indici vengono correlati, mediante un'apposita matrice di possibilità, per ottenere il Tier minimo raccomandato.

Lo schema complessivo di calcolo del modello è riassunto nella seguente figura, dove sono rappresentati:

- in verde, i parametri inseriti dall'utente;
- in rosso, i parametri calcolati e non visualizzati (ad uso interno);
- in azzurro, i valori risultanti mostrati all'utente.



Il foglio di calcolo

Oltre alle pagine relative alle tre direttrici, il foglio elettronico predisposto come implementazione del modello comprende una prima pagina relativa alla descrizione generale dell'Amministrazione oggetto di autovalutazione ed una pagina contenente i risultati.

Parametri delle direttrici

Le tre direttrici indicate comprendono i seguenti parametri.

Direttrice del servizio

La direttrice del servizio, implementata nella seconda pagina di lavoro del foglio elettronico, comprende i seguenti parametri:

Parametro
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
E' possibile recuperare la mancata acquisizione dei dati
E' 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

Direttrice dell'organizzazione

La direttrice dell'organizzazione, implementata nella terza pagina di lavoro del foglio elettronico, comprende i seguenti parametri:

Parametro
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

Direttrice della tecnologia

La direttrice della tecnologia, implementata nella quarta pagina di lavoro del foglio elettronico, comprende i seguenti parametri:

Parametro
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

Dati di sintesi e risultati finali

Nella quinta pagina di lavoro del foglio elettronico sono riportati i dati di sintesi elaborati dal foglio, sulla base dei valori che vengono inseriti in corrispondenza dei parametri sopra riportati.

Il dato di sintesi fondamentale che viene elaborato è l'*Indice complessivo di criticità* che è la risultante delle tre direttrici *servizio, organizzazione, tecnologica.*

Sulla base del valore che assume, l'Indice di criticità determina una delle 4 classi di criticità: Bassa, Media, Alta, Critica.

La valutazione della Soluzione tecnologica (Tier) viene operata in questo modo: da un sottoinsieme dei parametri della dimensione del servizio, relativi alla valutazione di RTO ed RPO, viene derivato un indice interno di criticità RTO+RPO il quale viene correlato con l'indice della dimensione della tecnologia per derivare la Soluzione tecnologica minima raccomandata (Tier).

Si precisa che relativamente alle possibili alternative associate al parametro "Tipo di dati trattati", presente nella direttrice dei servizi, sono stati attribuiti nello strumento pesi progressivi crescenti come segue:

- Dati personali;
- Dati sensibili e giudiziari;
- Dati legati alla salute e alla vita sessuale.

Le tabelle e gli esiti del percorso di autovalutazione, come si è già avuto modi di evidenziare nei capitoli 5 e 7, vanno inviati a DigitPA, in formato elettronico, in allegato allo Studio di Fattibilità Tecnica.

APPENDICE D: POSSIBILI REQUISITI DEL SITO DI DR

Nella presente appendice, in linea con le considerazioni espresse nel Capitolo 6 del presente documento si riportano, a titolo puramente esemplificativo, alcuni requisiti che un sito di DR dovrebbe poter soddisfare al fine di ospitare i servizi di Disaster recovery, tenuto conto dello stato dell'arte dei moderni datacenter e delle normative tecniche, degli standard esistenti al riguardo e dei requisiti definiti per le soluzioni.

Requisiti generali e inerenti alla localizzazione del sito

R.1.01	Il sito dovrà avere un'opportuna distanza in linea d'aria dal sito primario, ove risiede il sistema Informativo dell'Amministrazione. Ove sia richiesta una soluzione con modalità di aggiornamento sincrono, allo stato attuale della tecnologia nell'individuare la distanza e la localizzazione del sito, non si può prescindere dalle caratteristiche della connettività sia in termini di distanza che di latenza, in quanto la "sincronizzazione", non è possibile al di sopra di certe distanze fisiche fra sito primario e secondario
R.1.02	Le aree adibite ad ospitare i sistemi di ripristino devono essere dislocate su di un unico sito
R.1.03	Il sito dovrà essere in regola con tutte le concessioni edilizie ed i permessi rilasciati dagli uffici competenti del Comune sul quale sorge lo stesso.
R.1.04	Qualora il sito di DR sia costruito su territorio soggetto ad attività sismica, lo stesso deve avere una struttura progettata per minimizzare gli impatti dell'onda sismica, attraverso la riduzione del numero di piani, il consolidamento dei piani inferiori e l'utilizzo di materiali di alta qualità, che possano resistere alle vibrazioni provocate dal sisma e che prendano fuoco difficilmente. Pertanto, si richiede l'attestato di valutazione di rischio sismico coerente con la l'area geografica che ospita il sito.
R.1.05	Il sito di DR non deve essere localizzato in una regione affetta da tempeste di ghiaccio e neve.
R.1.06	Il sito di DR non deve essere localizzato in aree soggette ad allagamenti e/o alluvioni.
R.1.07	Il sito di DR non deve essere localizzato in aree soggette a frane.
R.1.08	Il sito di DR non deve essere localizzato vicino ad aeroporti, centrali elettriche o stazioni di scambio ferroviario per evitare il fenomeno di interferenza da emissioni elettromagnetiche
R.1.09	Il sito di DR deve avere un impianto con luci di emergenza, completo di linee di distribuzione ed opportunamente sezionato con interruttori magnetotermici differenziali al quadro elettrico, deve avere una configurazione composta da corpi illuminanti stagni IP 44 in materiale termoestinguente, con led di segnalazione di presenza di rete, cablate con lampade da 18 W, con batterie tampone in grado di garantire un minimo di 3 ore di funzionamento in caso di mancanza di tensione.
R.1.10	Il sito di DR deve avere un impianto di illuminazione primaria completo di linee di distribuzione, interruttori ed opportunamente sezionato con interruttori magnetotermici differenziali al quadro elettrico, in grado di garantire su tutta la superficie utile del sito un illuminamento a "tutto acceso" pari a 600 Lux.

R.2.01	Il pavimento antistatico soprelevato dovrà avere una altezza utile non inferiore a cm 25 con supporto di carico distribuito superiore a 2.500 Kg/mq e carico di punta pari o superiore a 500 Kg.
R.2.02	La soletta dovrà essere in grado di supportare carichi di almeno 500 Kg/mq, evidenziata da relativa certificazione di collaudo rilasciata da ente o professionista abilitato. Le solette dovranno essere opportunamente sigillate al fine di garantire l'adeguata resistenza al fuoco e prevenire la circolazione di polvere.
R.2.03	Il pavimento flottante dovrà avere una struttura modulare con modulo 60 cm x 60 cm, resistenza al fuoco minima pari a REI 60 e spessore minimo pari a circa 4 cm.
R.2.04	L'altezza utile dal pavimento flottante dovrà essere di almeno 270 cm.
R.2.05	Presenza di sensore installato sulla pavimentazione esistente sotto il pavimento flottante, in grado di rilevare il liquido ad una altezza variabile tra 0 ed 11 millimetri. Tale dispositivo dovrà avere funzioni di test e di inibizione da remoto, oltre alla possibilità di regolazione della soglia di allarme. Grado di protezione IP 67.
R.2.06	Presenza di punti manuali di attivazione degli allarmi dotati di dispositivo di isolamento dai cortocircuiti sulla linea di rilevazione, attivabili mediante azione su lastra di vetro con punto di rottura e azionamento pulsante.
R.2.07	Presenza di segnalatori acustici installati, in concomitanza a segnalatori luminosi di allarme, con potenza sonora di 95 dB, indicanti almeno le seguenti condizioni: "ALLARME INCENDIO", "SPEGNIMENTO IN CORSO", "ALLARME EVACUAZIONE", "ALLARME ALLAGAMENTO".

R.2.08	Aree separate dalle altre mediante parete “slab to slab” a contenimento di fuoco, tali da garantire una resistenza al fuoco di almeno 2 ore e sigillate in corrispondenza di ogni attraversamento. L’accesso a questa area deve avvenire mediante porta con chiusura automatica e a contenimento di fuoco.
R.2.09	Il tetto dell’edificio deve essere dotato di idoneo sistema di drenaggio delle acque piovane, di idoneo sistema di impermeabilizzazione senza la presenza di membrane in PVC, e di un facile sistema di manutenzione ed accesso al fine di presentare il minor numero possibile di aperture destinate agli impianti di supporto al centro.
R.2.10	Presenza, all’interno dello stesso complesso edilizio e comunque a non oltre 1 km in linea d’aria dai locali ospitanti le risorse elaborative e di storage, di almeno ottanta postazioni di lavoro e di almeno una sala riunioni attrezzata, per ospitare il personale dell’Amministrazione interessata in occasione dei test/collaudo e in condizioni di emergenza.

Requisiti inerenti gli impianti del sito

R.3.01	L’alimentazione elettrica dell’infrastruttura ICT destinata a ripristinare i sistemi dovrà essere garantita da sistemi ridondati ed in parallelo costituiti da gruppi elettrogeni e sistemi UPS a garanzia dell’erogazione con continuità e qualità dell’alimentazione elettrica (continuità di erogazione e qualità della tensione) a fronte di guasti e/o distacchi (programmati o no) a carico della rete di distribuzione.
R.3.02	Presenza di almeno 2 gruppi di continuità (UPS) in configurazione parallela ridondata ed aventi batterie con autonomia di almeno 10 minuti a pieno carico e comunque congruo per l’attivazione del sistema di emergenza. Gli UPS dovranno assicurare la continuità a tutti i dispositivi informatici e l’illuminazione d’emergenza. I locali UPS e Batterie devono essere adeguatamente compartimentati con canalina di contenimento di eventuali fuoriuscite di liquidi, da sistema di condizionamento e, nel caso di batterie elettrolitiche, da sistema di espulsione gas e da rilevatori idrogeno.
R.3.03	Il sito deve essere in grado di operare in assenza di utilities esterne (acqua, gas, luce, etc.) per un periodo di tempo pari a 48 ore senza rifornimenti.
R.3.04	Nel caso di interruzioni superiori alle 48 ore deve essere previsto un piano di approvvigionamento alternativo, da quello della rete di distribuzione usuale, con fornitori terzi; in particolare per il carburante destinato ai gruppi elettrogeni.
R.3.05	Presenza di una doppia sorgente di alimentazione elettrica per i rack e/o i server installati. Le due linee di alimentazione devono essere mantenute entrambe attive anche durante gli interventi di manutenzione programmata mediante apposite operazioni di switch. Si richiede inoltre la presenza di static switch automatici in grado di ovviare ad una caduta su una delle due linee di alimentazione con trasferimento automatico del carico sulla seconda linea. Questi switch dovranno essere posizionati a livello dei quadri di piano o di sala.
R.3.06	Per quanto attiene le aree IT e TLC la distribuzione dovrà essere realizzata con doppio circuito di blindo-sbarre o cavi elettrici, a seconda del livello di distribuzione con diversi livelli di selettività al fine di evitare la propagazione del corto circuito, alimentate/i da quadri elettrici separati. Relativamente all’area TLC, si richiede la presenza di una adeguata infrastruttura di telecomunicazione destinata ad ospitare gli apparati necessari per i collegamenti WAN e a garantire l’attestazione dei collegamenti SPC.
R.3.07	Presenza di switch dell’alimentazione dei condizionatori di sala per consentire il passaggio automatico alla seconda linea di alimentazione in caso di caduta sulla prima. Le caratteristiche richieste sono le seguenti: o tensione di alimentazione a 400 Volt 3F e 240 Volt MF; o potenza media minima erogabile 0,5 KVA/mq (solo carico IT) con possibilità di incremento a 0,8 KVA/mq; o utenze sezionabili con interruttori automatici magnetotermici e con salvavita; o anello di terra unico (equipotenzialità). Pulsante di sgancio manuale (Emergency Power Off) dove necessario.
R.3.08	Presenza di impianto di condizionamento del sito di DR ridondato con sensori per il controllo della temperatura e dell’umidità.
R.3.09	Sistema di monitoraggio continuo della temperatura nell’area del datacenter attraverso sensori per la segnalazione dell’allarme connesso al superamento delle temperature ammesse per il corretto funzionamento delle macchine all’interno del datacenter.
R.3.10	Presenza di impianto di condizionamento adeguato a garantire la piena operatività degli apparati di ripristino anche in caso di guasto alle singole componenti dell’impianto (sia relativamente alla distribuzione che relativamente alle unità di condizionamento).

R.3.11	Sistema di rilevazione anti incendio costituito da rilevatori di fumi e calore in grado da allarmare il personale di sorveglianza e attivare automaticamente gli impianti di spegnimento.
R.3.12	Presenza di impianto di rilevazione fumi progettato nel pieno rispetto della normativa UNI 9795 con garanzia della segmentazione dello stesso e la conseguente perdita delle sole zone oggetto di eventuale manutenzione, incidente o calamità naturale, ma con il continuo funzionamento del resto dell'impianto.
R.3.13	Sistema di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso di tipo ARGON o altri gas non alogenati. L'impianto deve permettere di controllare più focolai contemporanei, evitando invasioni di fumo, sbalzi improvvisi di temperatura e dispersione di residui nocivi per l'uomo e per le apparecchiature. L'efficacia delle bombole o serbatoi dell'estinguente dovrà essere verificata in accordo con le norme vigenti. La collocazione delle bombole dovrà essere in locale separato dell'edificio.
R.3.14	Previsione di un adeguato sistema di bonifica dei locali "a scarica di gas avvenuta" per permettere il riutilizzo dei locali in breve tempo.
R.3.15	Monitoraggio 24hX7 degli impianti.

Requisiti per la sicurezza del sito

R.4.01	I locali adibiti ad ospitare le infrastrutture di ripristino devono essere conformi a quanto previsto dalle attuali norme sulla sicurezza e salute sul luogo di lavoro dei lavoratori, di cui al DLgs.. n. 81/2008 e s.m.i.
R.4.02	Predisposizione di aree sicure dotate di appropriate barriere di sicurezza controllate tramite apposito sistema di videosorveglianza.
R.4.03	Accesso al sito regolato e controllato da procedure di riconoscimento e registrazione effettuato presso la reception.
R.4.04	Monitoraggio dell'ingresso principale attraverso telecamere a circuito chiuso con registrazione continua o attivabile attraverso sensore di movimento anche IR.
R.4.05	Protezione interna tramite sistema di telecamere a circuito chiuso.
R.4.06	Accesso alle sale macchine mediante identificazione/autenticazione attraverso un controllo elettronico e/o riconoscimento biometrico.
R.4.07	Sistema antintrusione che consenta di rilevare la presenza di persone all'interno delle aree sensibili.
R.4.08	Protezione esterna tramite sistema antiscavalcamento con illuminazione perimetrale, sistema di rilevamento presenza e telecamere a circuito chiuso controllate dal personale di sicurezza 24 ore su 24.

Requisiti per la Sicurezza interna e l'accesso all'edificio del sito

R.5.01	Identificazione di uno o più responsabile/i delle aree del sito per le autorizzazioni necessarie all'accesso.
R.5.02	Procedura di accesso alle aree per limitare l'accesso alle persone autorizzate dal responsabile, con almeno le seguenti classi di accesso: o personale del prestatore, o personale clienti del prestatore, o personale delegato dal prestatore (ad esempio personale che esegue manutenzione/riparazione, ecc.). La procedura deve anche regolare la gestione di badge/passi temporanei e le modalità di accompagnamento di personale esterno (clienti, manutenzione, ecc.) alle varie aree del sito da parte di personale del prestatore.

Altre caratteristiche

R.6.01	Presenza di aree ristoro nei piani che ospitano le postazioni di lavoro
R.6.02	Disponibilità di locale di pronto soccorso.
R.6.03	Conformità alle disposizioni in merito alla organizzazione del pronto soccorso aziendale, alla formazione degli addetti al pronto soccorso ed alle attrezzature necessarie per effettuare gli interventi di primo soccorso e gestione dell'emergenza sanitaria.

APPENDICE E: ESEMPI DI LIVELLI DI SERVIZIO

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**	**Ambito di applicabilità dell'adempimento /indicatore; soluzione e casi cui si può adattare**
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 e 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. Le penali saranno applicate per tutto il tempo per il quale si prolunghi l'inadempienza a far data dal giorno nel quale sarà stata formalizzata la contestazione e fino al giorno nel quale il fornitore porrà fine all'inadempienza	Ambito di applicabilità abbastanza generale; assicura la tempestività di consegna dei deliverable; si può adattare a qualsiasi soluzione tecnica di DR scelta
Dare avvio al servizio richiesto nei tempi e correttamente	Mancato/tardato avvio del contratto rispetto ai termini previsti	Giorno solare	Verificare che le attività e servizi richiesti risultino avviati e completati nei tempi e correttamente	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 e per tutto il tempo per il quale si prolunghi	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. E' anche opportuno distinguere il mancato avvio del servizio in generale dal mancato avvio/

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	Ambito di applicabilità dell'adempimento /indicatore; soluzione e casi cui si può adattare
				l'inadempienza a far data dal giorno nel quale sarà stata formalizzata la contestazione e fino al giorno nel quale si verificherà che il fornitore ha posto fine all'inadempienza, avviando/completando i servizi e le attività contrattuali	completamento delle attività comprese nel servizio ad es. graduando la penalità in considerazione dell'importanza dell'attività non svolta, avviata/completata tardivamente
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 sia 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 svolgi-mento 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
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).	Perdita dati superiore ai valori e inconsistenza dei dati di copia/backup	Percentuale Es. un RPO tale che il 99% dei dati copiato nella finestra temporale prevista sia correttamente effettuato e sia allineato ai dati	Nella finestra temporale prevista per il monitoraggio dell'indicatore verranno effettuati dei campionamenti ad intervalli di tempo predefiniti. Es. se la finestra è giornaliera	Per ogni punto percentuale di scosta-mento 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	Ambito di applicabilità generale; è un indicatore essenziale alla verifica del corretto svolgimento del servizio di DR. Va definito tenuto conto del contesto

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	Ambito di applicabilità dell'adempimento /indicatore; soluzione e casi cui si può adattare
Va rispettato e verificato periodicamente, in occasione dei test/simulazioni di disaster e in caso di attivazione della configurazione di emergenza.		del sistema primario	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: ∆ percentuale = (NT – N fuori soglia)/ NT * 100 >/= 99 %	complessivo previsto	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 tem-pestività di ripristino in caso di guasto, malfunzio-namento o ano-malie di tutte le componenti, anche ridondate, del servizio di DR, assicurandone la manutenzione e la perfetta efficienza. 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 ri-pristino de-finiti e pari a : -….h/giorni solari, in condizio-ni normali; -….h/giorni solare in con-dizioni di emer-genza, a decorrere dal momento della segnalazione co-munque pervenuta.	DOS – DORipr. = 0 Ove: -DOS = Data e ora di segnalazione del guasto, malfunzionamento/an omalia -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, rispettiva-mente, 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/apert ura 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.
Garantire la disponibilità delle risorse e componenti necessarie alla soluzione di DR previste	Indisponibilità del numero e tipologia delle risorse previste e necessarie	% / nr. di risorse effettiva-mente disponibili (per numero e	Risorse Previste nel mese di riferimento – Risorse Disponibili nel mese di riferimento	Per ciascun caso di inadempimento (numero in meno o punto percentuale in	Da prevedere quando si sia espressamente richiesta la

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	Ambito di applicabilità dell'adempimento /indicatore; soluzione e casi cui si può adattare
	all'eroga-zione dei servizi di DR che possano avere impatto sulla soluzione di DR richiesta	tipologia) es. nella finestra temporale mensile	Risorse Previste nel mese di riferimento	meno rispetto alla soglia prevista/al numero e tipologia di risorse, verrà applicata una penale pari, rispettiva-mente, 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	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 ed eventualmente monitoraggio da remoto.
Garantire la disponibilità degli spazi richiesti (in termini di MQ e caratteristiche e requisiti)	Indisponibilità/inadeg uatezza 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 quando si sia espressamente richiesta la disponibilità di un certo tipo e numero di spazi (housing). Può esser anche un aspetto che attiene alla fase di collaudo e test della soluzione e ricadere quindi negli adempimenti affidati al fornitore per il superamento del collaudo o del test
Assicurare il tempestivo e corretto svolgimento dei	In caso di ritardata esecuzione dei test	Giorno solare di ritardo	Riscontro del ritardo/mancata	Per ogni giorno solare di ritardo nell'ese-	Ambito di applicabilità

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	Ambito di applicabilità dell'adempimento /indicatore; soluzione e casi cui si può adattare
test periodici. I test periodici dovranno essere svolti nel rispetto dei termini previsti, in modo adeguato e rispondente a quanto prescritto dal piano di continuità/DR	periodici		esecuzione del test per cause imputabili al fornitore.	cuzione dei test, sarà applicata una penale pari allo XXX % del corrispettivo complessivo mensile previsto	generale; è un indicatore essenziale alla verifica del corretto svolgimento del servizio di DR.
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. 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.
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	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	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	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

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	Ambito di applicabilità dell'adempimento /indicatore; soluzione e casi cui si può adattare
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	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.			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.	effettuare delle verifiche di conformità sul corretto svolgimento del servizio di DR.
Garantire - sia in caso di sostituzione o aggiornamento 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 certificata dei dati contenuti negli apparti usati per la soluzione di CO/DR. Garantire la cancellazione delle flash 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 inadempienza e per ciascun giorno di contestata inadempienza	Verificato che la cancellazione delle flash copy utilizzate per il test, al termine dello stesso e che la cancellazione certificata dei dati dallo storage o da parti di esso non risulti effettuata o 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	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'Amministra-zione che fruisce del servizio di DR. Rende opportuno definire come verificare l'avvenuta cancellazione

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	Ambito di applicabilità dell'adempimento /indicatore; soluzione e casi cui si può adattare
			termine del contratto – sarà applicata la penale prevista conteggiando tutti i giorni per cui perduri la situazione di non conformità contestata		
Assicurare che le risorse professionali messe a disposi-zione 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 particolare per l'Amministrazione che fruisce della soluzione di DR. Rende opportuno definire il mix che si richiede e prevede-re strumenti di verifica e controllo delle risorse messe a disposizione.