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:

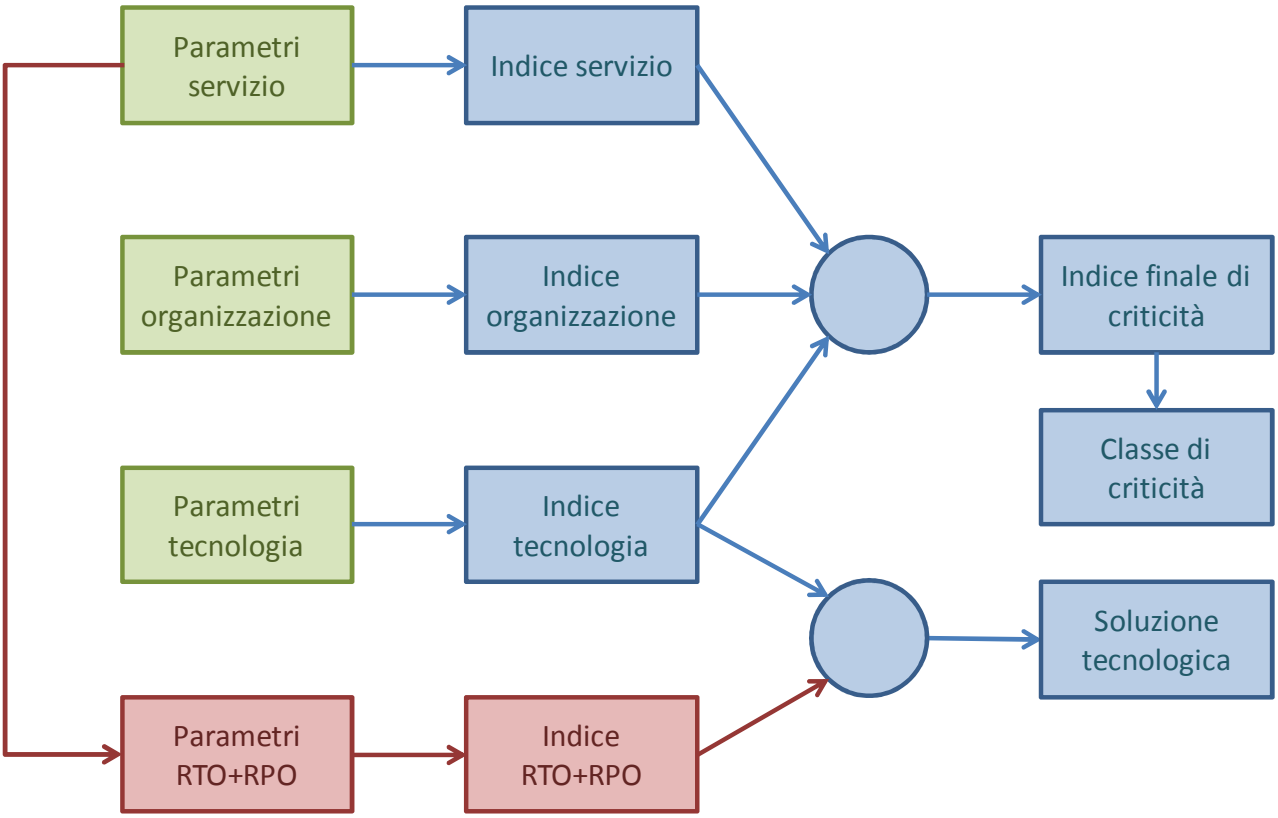
$$I = \frac{\sum_i p_i v_i}{\sum_i p_i}$$

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/