

Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione

Manuale operativo

Dizionario delle Forniture ICT

Classe di Fornitura

Continuità Operativa COP

INDICE

1 GENERALITÀ SUL DOCUMENTO..... 3

2 DESCRIZIONE DELLA CLASSE DI FORNITURA..... 4

3 MODALITÀ DI DEFINIZIONE DELLA FORNITURA 5

3.1 GENERALITÀ E MODALITÀ DI GESTIONE CONTRATTUALE..... 5

3.2 OBIETTIVI..... 8

3.3 UTENZA.....10

3.4 DIMENSIONE.....11

3.5 VINCOLI E REQUISITI.....12

3.6 STANDARD E NORME APPLICABILI.....12

3.7 RELAZIONI CON ALTRE CLASSI DI FORNITURA E MANUALI.....15

4 MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA.....16

5 DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI18

5.1 QUADRO COMPLESSIVO18

5.2 ANALISI E PIANIFICAZIONE PER LA CONTINUITÀ OPERATIVA20

5.3 EROGAZIONE DEL SERVIZIO: IMPLEMENTAZIONE24

5.4 EROGAZIONE DEL SERVIZIO: GESTIONE E MANUTENZIONE DEL SERVIZIO29

5.5 EROGAZIONE DEL SERVIZIO: GESTIONE E MANUTENZIONE STRAORDINARIA34

6 DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI.....36

7 INDICATORI/MISURE DI QUALITÀ42

8 GLOSSARIO51

1 GENERALITÀ SUL DOCUMENTO

Questo documento descrive uno dei lemmi del Manuale operativo “Dizionario delle forniture ICT” delle Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione. Ogni lemma del Dizionario rappresenta una classe di fornitura ICT elementare. Il Dizionario contiene tutte le classi di forniture che si sono ritenute necessarie per rappresentare compiutamente i contratti ICT delle pubbliche amministrazioni. Ogni lemma del Dizionario è autoconsistente e indipendente; esso prevede:

- **la descrizione della classe di fornitura ICT elementare**, che ha lo scopo di definirne univocamente l'ambito di applicazione;
- **l'esplicitazione di “regole” per l'uso della classe di fornitura**, utile a proporre al lettore suggerimenti sull'uso del lemma per la stesura dell'oggetto contrattuale;
- **la descrizione delle attività** relative alla classe di fornitura e dei relativi prodotti, utile al lettore come traccia riutilizzabile per scrivere contratti e capitolati tecnici;
- **una tabella che riassume attività, prodotti e indicatori di qualità**, utile al lettore come quadro sinottico che riassume il legame tra attività e relativi prodotti da queste realizzati ed identifica, in relazione ad entrambi, gli indicatori di qualità adottati per la classe di fornitura;
- **una scheda per ogni indicatore di qualità** (presente nella tabella di cui sopra), utile al lettore come traccia riutilizzabile, per scrivere contratti e capitolati tecnici;
- **un glossario** (ove necessario, e previsto nel presente lemma) specifico per la classe di fornitura.

Nell'ambito della complessa attività di scrittura di contratti e capitolati tecnici, i lemmi possono essere intesi come “ricette contrattuali” di immediato utilizzo mediante processi di copia e incolla, per rappresentare le esigenze della stazione appaltante.

Nell'ottica del riuso, particolare attenzione dovrà essere prestata alle imprescindibili e necessarie attività di specificazione e taratura delle classi di fornitura ICT elementari utilizzate e, successivamente, all'integrazione delle diverse classi di fornitura scelte in un unico e coerente contratto ICT.

La versione digitale di ogni lemma è singolarmente scaricabile dal sito CNIPA in formato editabile (.rtf) che ne permette il riutilizzo anche parziale.

Per maggiori informazioni sull'utilizzo integrato delle classi di fornitura e dei processi trasversali si rimanda agli esempi contenuti nel Manuale applicativo “Esempi di applicazione”.

I contenuti del presente lemma traggono origine dai risultati raggiunti dal centro di competenza promosso dal CNIPA a favore della formazione e della promozione della continuità operativa nel settore pubblico.

Il Gruppo di Lavoro costituito da CNIPA – al quale sono stati invitati a partecipare le pubbliche amministrazioni centrali e locali, i rappresentanti dei fornitori ed altri soggetti istituzionali interessati – ha realizzato tra gli altri risultati il documento “Linee Guida alla Continuità Operativa nella Pubblica Amministrazione”, le cui conclusioni sono alla base della Classe di fornitura ivi presentata.

2 DESCRIZIONE DELLA CLASSE DI FORNITURA

La classe di fornitura "Continuità Operativa" (COP) comprende le attività necessarie per valutare, progettare, implementare e gestire gli obiettivi di continuità operativa dei servizi informatizzati della pubblica amministrazione centrale e locale.

Con il termine continuità operativa nella pubblica amministrazione si intende l'insieme dei metodi e degli strumenti finalizzati ad assicurare la continuità dei servizi istituzionali e delle relative procedure amministrative anche in presenza di eventi o condizioni che possono causare il fermo prolungato dei sistemi informatici a supporto parziale o totale dei servizi stessi.

La pubblica amministrazione deve assicurare la continuità dei propri servizi di maggiore rilevanza così da garantire il corretto svolgimento della vita nel Paese anche in presenza di eventi catastrofici o comunque tali da determinare l'interruzione dei servizi per un periodo di tempo prolungato.

La necessità di garantire la continuità dei servizi è dettata in linea generale dall'art.97 della Costituzione e dal principio di buon andamento dell'amministrazione, da rispettare anche se si utilizzano tecnologie ICT. In particolare, sono in essere norme e direttive specifiche; si vedano, ad esempio:

- la Direttiva 16/01/2002 recante "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali;
- il Codice in materia di protezione dei dati personali (D.L. 196 30/06/2003);
- il D.P.C.M. 31/05/2005 (G.U. 18/06/2005, n.140).

Anche la continuità dei servizi informatici rappresenta quindi 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.

Rientrano nella disciplina della continuità operativa dei servizi ICT quegli eventi che procurano danni imprevisti, difficilmente fronteggiabili con strumenti e procedure d'uso quotidiano, e tali da esporre palesemente la pubblica amministrazione al rischio di indisponibilità delle funzioni informatiche per un periodo di tempo prolungato (o comunque non compatibile con le finalità del servizio stesso).

Data la vasta applicabilità su diverse casistiche, è conveniente stabilire un perimetro della continuità operativa in quanto insieme di attività che presentano caratteristiche omogenee per finalità e modalità di realizzazione e gestione.

A tal fine, le finalità della continuità operativa sono distinte dalle finalità di risoluzione problemi che rientrano nell'ambito della qualità dei prodotti e dei servizi informatici (ad es. errori di progettazione, di configurazione, malfunzionamenti di componenti hardware o software), o nell'ambito della sicurezza informatica (ad es. eventi di tipo accidentale o malevolo che determinano l'interruzione di alcune applicazioni).

Qualche esempio potrà chiarire meglio questo aspetto. 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'innescò 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.

Si osservi che le attività specifiche della fornitura possono essere ripetute - per finalità e livelli di approfondimento diverso - in più di una delle fasi che definiscono la fornitura stessa, la quale si caratterizza di base come fornitura di servizi. L'amministrazione può scegliere se includere la fornitura di beni (es. sistemi informatici) o se acquisire i beni necessari alla soluzione di continuità operativa separatamente dalla acquisizione del servizio.

3 MODALITÀ DI DEFINIZIONE DELLA FORNITURA

3.1 GENERALITÀ E MODALITÀ DI GESTIONE CONTRATTUALE

La classe di fornitura "Continuità Operativa" viene articolata in due istanze:

- Analisi e Pianificazione per la Continuità Operativa
- Erogazione del servizio

La modalità di acquisizione della fornitura è quella della consulenza per quanto riguarda la prima istanza (Analisi e Pianificazione) e quella della fornitura di servizio per l'istanza di "Erogazione" (es. *outsourcing*).

L'istanza "Analisi e Pianificazione" raccoglie quelle attività di analisi e di progettazione di massima che nella letteratura della Continuità Operativa (*Business Continuity*), sono indicate principalmente dalle fasi di analisi del rischio (*Risk assessment*) e di valutazione di impatto sull'operatività (*Business impact analysis*).

L'istanza "Erogazione del Servizio" segue temporalmente e funzionalmente l'analisi e la pianificazione. Essa è costituita dalle attività di costituzione del servizio di continuità operativa e, quindi, dalle attività di gestione e manutenzione dello stesso, che includono tutte le attività di adeguamento della soluzione di continuità operativa alle modifiche ed ai cambiamenti del sistema informatico per la durata contrattuale del servizio di continuità operativa.

Sono ugualmente incluse in questa istanza le attività di test periodico della soluzione di continuità e di aggiornamento del Piano di Continuità.

In pratica, le attività previste in questa istanza sono attivate dalle attività di gestione del cambiamento ICT e dai risultati dei test periodici.

In caso di evento disastroso, l'istanza include anche il ripristino del servizio informatico secondo le procedure e le responsabilità definite nel Piano di Continuità.

Nel seguito, ognuno degli elementi caratterizzanti l'oggetto contrattuale tratta singolarmente le due istanze; nella prassi, è cura della amministrazione includere le due istanze della Classe di Fornitura in un unico oggetto contrattuale, oppure prevedere un oggetto contrattuale per ogni istanza.

Ogni singola amministrazione - ovvero più amministrazioni associate in una delle forme di collaborazione attuabili -, potrà individuare al meglio la modalità di gestione contrattuale (contratto unico per entrambe le istanze o contratti separati), attraverso la valutazione di due principali elementi:

- il livello di delega operativa, legato alla capacità di gestione contrattuale;
- l'ampiezza e la tipologia di attività affidate (in funzione di esigenze differenziate di continuità operativa dei servizi erogati dall'amministrazione).

L'amministrazione può determinare il proprio livello di delega operativa, valutando la propria capacità in termini di risorse organizzative e di competenza. In generale, l'amministrazione dovrà dotarsi di risorse adeguate per seguire e controllare l'esecuzione del contratto sia nelle fasi di gestione ordinaria del servizio, sia nelle fasi di gestione straordinaria (in caso, cioè, di avvenuto disastro); tale controllo (*governance*) può essere svolto a più livelli, dove il livello minimo è quello del controllo di conformità dell'esecuzione alle specifiche contrattuali, ed il livello massimo è quello del periodico aggiornamento e miglioramento del servizio.

Il livello massimo richiede l'introduzione di elementi di flessibilità contrattuale specifici e, quindi, richiede all'amministrazione di dotarsi di competenze specifiche nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI, in Inglese ISMS – Information Security Management System, definito dallo standard ISO17799:2005).

Un ulteriore esempio a riguardo del livello di delega operativa, può essere dato alle amministrazioni, nel merito di alcune attività tipiche della gestione operativa ordinaria del servizio della continuità operativa. Tra queste possono essere ricordate le attività di monitoraggio diretto del funzionamento dei meccanismi di protezione dei dati messi in campo (es. replica remota) e le attività di allineamento delle configurazioni dei sistemi tra il sito primario ed il sito di recovery. Lo svolgimento di tali attività – e di altre eventuali - richiede un adeguamento della capacità organizzativa dell'amministrazione.

Se si assimila l'erogazione del servizio di continuità operativa a quella di un contratto di outsourcing della durata di 3-5 anni (o più), si vede che il contratto stesso dovrà prevedere quegli elementi tipici di flessibilità tali da consentire la gestione dei cambiamenti e la conseguente variazione dei costi economici annuali.

Nel caso di forma contrattuale unica per le due istanze, i cambiamenti saranno quindi legati essenzialmente a tre eventi:

- il cambiamento del sistema informativo (es. nuovi progetti, ma anche revisione di procedure e nuove procedure);
- la revisione del Piano di Continuità (a valle ad es. dei risultati dei test periodici semestrali o annuali);
- il risultato delle attività previste nell'istanza di Analisi e Pianificazione.

Dal punto di vista della stesura del capitolato, l'amministrazione raccoglierà in uno studio di fattibilità di alto livello i macro elementi che caratterizzano la continuità operativa:

- ambito di intervento in termini di procedure amministrative e di sistemi informatici;
- stima di massima dell'impatto della non disponibilità del sistema informatico nel tempo, (es. a 1 giorno, 1 settimana, 1 mese);
- macro-obiettivi di continuità;
- modalità generali di intervento a supporto della continuità operativa;
- stima economica dell'intervento.

Questo approccio consente all'amministrazione di indirizzare e prevedere nel servizio proposto dal Fornitore due temi critici della Continuità Operativa:

- l'esigenza di gestire il cambiamento (tecnologico - relativo alle risorse informatiche ed organizzative – relativo alle procedure amministrative) nel corso della erogazione del servizio e quindi l'esigenza di introdurre nel rapporto committente/fornitore elementi di flessibilità contrattuale;
- un approccio ciclico, per fasi ed evolutivo all'implementazione della continuità operativa, potendo segmentare le istanze di analisi ed erogazione, in interventi successivi con impatto di minor rischio e complessità (tipicamente in base alle priorità di continuità dei servizi e delle procedure amministrative più critiche).

Si osservi che l'approccio con contratto unico per entrambe le istanze può risultare di gestione troppo onerosa per le amministrazioni dotate di un sistema informatico di complessità medio-bassa e poco soggetto a cambiamenti. In tal caso, l'approccio con contratti distinti può risultare più adeguato. In questa situazione può essere conveniente eseguire l'istanza di Analisi e Pianificazione in un contesto di specializzazione dello Studio di Fattibilità.

Le amministrazioni di struttura medio-piccola con sistemi informatici e procedure che cambiano con bassa frequenza, possono trovare più favorevole percorrere la fase di analisi separatamente da quella di erogazione. Ciò anche in un contesto di erogazione del servizio di continuità operativa secondo modalità di "mutuo soccorso" sulla base di accordi con altre amministrazioni: separando la fase di analisi da quella di erogazione, più amministrazioni potranno opportunamente valutare l'efficacia degli accordi reciproci di "mutuo soccorso" sulla base dei risultati della fase di analisi.

Le amministrazioni di struttura medio-grande sono in genere caratterizzate da sistemi informatici complessi più frequentemente soggetti a cambiamenti nelle procedure e nelle tecnologie, con l'esigenza di rivedere spesso i risultati dell'analisi. Queste amministrazioni potranno trovare più favorevole impostare l'intervento attraverso un contratto unico, che includa sia la parte di analisi, sia la parte di erogazione del servizio – prevedendo inoltre che la fase di analisi possa essere ripetuta periodicamente attraverso opportuni meccanismi di attivazione da prevedere tra le attività di erogazione (si veda nel seguito quali eventi possono determinare la revisione della fase di analisi, che si realizza nell'aggiornamento del Piano della Continuità Operativa).

Un caso da menzionare a parte è quello in cui l'amministrazione abbia affidato a terzi (es. outsourcer, che nel caso è definito "primario") la gestione operativa dei sistemi informatici oggetto della continuità operativa (sia esso un affidamento totale, od anche parziale, come accade ad es. nel caso di fornitura del servizio di rete SPC).

In questo caso specifico, l'amministrazione dovrà prevedere l'adeguamento degli accordi di servizio con l'outsourcer "primario", sulla base dei requisiti di continuità operativa ed in

sostanza sulla base della soluzione adottata con il fornitore del servizio di continuità operativa (che nel caso è definito outsourcer “secondario”). Questo adeguamento è propedeutico alla esecuzione del servizio di continuità, e può essere definito nel dettaglio solo a valle della definizione del servizio di continuità operativa (ovvero quando la soluzione di continuità ed i relativi livelli di servizio siano ben definiti).

Ulteriori approfondimenti ed esempi sono disponibili nel documento “Linee Guida alla Continuità Operativa nella Pubblica Amministrazione”.

Le Linee Guida suggeriscono un percorso metodologico complessivo che è facilmente riconducibile alle attività in cui è articolata la classe di fornitura COP, come illustrato nella seguente tabella:

Linee Guida		Classe di Fornitura (COP)
Fase	Sottofase	Istanza
Analisi	Risk Assessment	Analisi e Pianificazione
	Business Impact Analysis	
	Recoverability Assessment	
Disegno	Strategia di continuità	
	Disegno della soluzione	
Realizzazione	Implementazione della soluzione	Erogazione del Servizio (Implementazione, Gestione del Servizio e Straordinaria)
	Gestione / Manutenzione	

3.2 OBIETTIVI

Il paragrafo presenta gli obiettivi specifici della classe di fornitura COP.

Obiettivi dell'istanza di Analisi e Pianificazione:

L'Analisi e la Pianificazione per la Continuità Operativa consente di raggiungere i seguenti obiettivi di gestione direzionale:

- acquisire adeguata ed effettiva consapevolezza sui requisiti di continuità operativa;
- ottenere una visione non solo puramente tecnologica dell'iniziativa, ma anche inclusiva degli obiettivi e dei benefici attesi, dei costi e dei rischi – realizzando così un quadro complessivo di riferimento per governare la complessità e per la verifica dei risultati;
- raccogliere tutti gli elementi essenziali per la definizione della fornitura del servizio di continuità operativa.

L'Analisi e la Pianificazione devono quindi avere una doppia valenza: decisionale sulla soluzione da adottare, e pratica di supporto nella stesura del capitolato relativo all'istanza di erogazione del servizio nella presente classe di fornitura.

Si hanno i seguenti obiettivi:

- la rilevazione dell'architettura corrente del sistema informatico (applicativa ed infrastrutturale);
- la valutazione del rischio (*Risk assessment*);

- l'analisi di impatto (dei rischi individuati) sull'operatività (*Business impact analysis*) e la determinazione degli obiettivi di continuità (RTO, RPO);
- la identificazione e valutazione tecnica di più strategie di ripristino (architetture tecnologiche per la realizzazione della continuità operativa);
- la determinazione e valutazione dei piani di massima (durata, risorse) dei progetti realizzativi associati alle strategie di ripristino individuate;
- la determinazione del piano formativo.

Obiettivi dell'istanza di Erogazione del Servizio:

Per facilitare la descrizione dell'istanza di Erogazione del Servizio, questa è suddivisa in tre fasi principali:

- Fase di Implementazione
- Fase di Gestione e Manutenzione del Servizio
- Fase di Gestione e Manutenzione Straordinaria

Fase di Implementazione:

- realizzare la soluzione di continuità individuata, attraverso la acquisizione dei beni e la predisposizione delle strutture, delle tecnologie e dei meccanismi di copia dei dati e di automazione (secondo i livelli definiti opportuni dall'amministrazione) della procedura di intervento;
- eseguire il piano di formazione;
- formalizzare, all'interno di un documento denominato "Piano di continuità operativa", le procedure operative da adottare con esplicitazione dei ruoli e delle responsabilità, negli scenari di crisi considerati (cioè indirizzati in fase di Risk assessment);
- collaudare le funzionalità infrastrutturali realizzate;
- collaudare il servizio di continuità operativa nel caso di evento disastroso (simulazione di crisi).

Fase di Gestione e Manutenzione del Servizio:

Le attività di gestione e manutenzione del servizio sono condotte generalmente su base periodica, in stretta relazione con le attività di gestione del cambiamento in area ICT. La periodicità di tali interventi è specifica di ogni singola amministrazione in funzione della criticità delle procedure, e della natura e della frequenza dei cambiamenti sia a livello organizzativo sia a livello componenti ICT.

Si hanno i seguenti obiettivi:

- garantire l'allineamento della soluzione di continuità rispetto all'evoluzione del sistema informatico e della struttura organizzativa dell'amministrazione;
- verificare il grado di preparazione complessivo (amministrazione e fornitore) nel rispondere e gestire situazioni di crisi, in accordo con quanto previsto dalla soluzione di continuità prescelta;
- verificare del livello di aggiornamento del Piano di continuità operativa in funzione dei cambiamenti ICT intercorsi;

- valutare l'adeguatezza del Piano di continuità operativa nel ripristino dell'operatività (simulazione di crisi);
- identificazione ed attuazione delle eventuali misure di adeguamento e/o miglioramento (interventi di tipo tecnologico, organizzativo, procedurale e/o formativo e di comunicazione).

Fase di Gestione della Crisi

Le attività di gestione e manutenzione straordinaria sono quelle attività che, in conformità con quanto prescritto nel Piano della Continuità, devono essere realizzate per garantire la continuità del servizio in caso di crisi, ovvero di dichiarazione di un evento disastroso.

Si hanno i seguenti obiettivi:

- esecuzione delle procedure e delle azioni previste nel Piano di Continuità: intervento per il ripristino della continuità operativa ("Intervento");
- gestione operativa straordinaria, ovvero gestione dei servizi informatici configurati per la continuità operativa, secondo i livelli di servizio pre-definiti in caso di crisi;
- esecuzione delle attività propedeutiche al rientro nelle condizioni di normalità.

3.3 UTENZA

La assicurazione della continuità operativa coinvolge un vasto bacino d'utenza, sia interno alla stazione appaltante, sia esterno.

Utenza interna

- Dipendenti e/o collaboratori amministrativi che si occupano dei procedimenti amministrativi rivolti a cittadini e/o imprese o dei procedimenti per il funzionamento dell'amministrazione; questi utenti possono essere coinvolti in particolare:
 - nelle attività di simulazione crisi (test periodici);
 - nelle attività di comunicazione e consapevolezza;
 - in attività di ricostruzione/reinserimento/validazione dei dati in sede di ripristino dopo evento catastrofico.
- Dipendenti e/o collaboratori tecnici informatici, che si occupano del funzionamento dei sistemi informatici dell'amministrazione; in particolare, sono individuati tra questi quattro ruoli ovvero gruppi organizzativi (la nomenclatura adottata nelle singole amministrazioni può variare):
 - Comitato di gestione della crisi;
 - Gruppo di supporto;
 - Gruppo di coordinamento tecnico;
 - Team di help desk (non necessariamente dedicato alla continuità operativa, ma con competenze specifiche).

Il Comitato di gestione della crisi è l'organo di direzione strategica ed ha responsabilità di garanzia e controllo sull'intero progetto; per questo è indicato a svolgere anche il ruolo di committente.

Utenza esterna

- Cittadini (in quando utenti finali di procedure e/o servizi, in particolare di servizi on-line)
- Imprese (in quando utenti finali di procedure e/o servizi, in particolare di servizi on-line)
- Fornitori (non solo i fornitori correnti, ma anche eventuali fornitori alternativi cui poter far ricorso in condizioni particolari; fornitori di connettività locale e geografica);
- Organizzazioni coinvolte in caso di crisi (es. Protezione civile, organi di Polizia, ecc.).

In considerazione del numero di ruoli utente coinvolti nell'iniziativa, viene fornita la tabella seguente come riferimento indicativo sulla articolazione degli utenti nei confronti delle attività di cui si compone la classe di fornitura.

(Il dettaglio relativo a ruoli ed organizzazioni nell'ambito dell'utenza tecnica informatica è indicato nel successivo Capitolo 5).

Utenza		Attività			
Tipologia	Ruolo / Organizzazione	Analisi e Pianificazione	Erogazione del Servizio		
			Implementazione	Gestione e Manutenzione del Servizio	Gestione e manutenzione straordinaria
Interna	Dipendenti e/o collaboratori tecnici informatici	●	●	●	●
Interna	Dipendenti e/o collaboratori amministrativi	◐	○	◐	●
Esterna	Fornitori (incluso eventuale outsourcer)	◐	●	●	●
Esterna	Organizzazioni di crisi	○	○	○	●

Legenda (indicatori del livello di impatto delle attività sui ruoli / organizzazioni elencati)	
○	Nessun impatto o impatto minimo
◐	Impatto parziale o circoscritto nel tempo
●	Impatto continuativo o comunque con periodicità di intervento significativa

3.4 DIMENSIONE

Le variabili di dimensionamento della fornitura che impattano su costi, rischi e qualità, possono essere così identificati:

Per l'istanza di "Analisi e Pianificazione":

- dimensione dell'amministrazione (organizzazione e numero di procedimenti);
- dimensione dell'organizzazione Sistemi Informativi;
- numero di referenti per le procedure amministrative;
- perimetro ICT (numero di componenti, inclusi i componenti di rete e desktop).

Per l'istanza di "Erogazione del servizio", oltre alle variabili di dimensionamento precedentemente illustrate per l'istanza di Analisi e Pianificazione:

- RTO (tempo di ripartenza);
- RPO (massimo intervallo di transazioni perse);
- versatilità della soluzione (cioè possibilità di utilizzo anche in condizioni di gestione ordinaria del servizio);
- qualità e sicurezza dei servizi in condizioni di emergenza;

- tempo massimo di permanenza in condizioni di emergenza;
- probabilità di recupero (ossia probabilità che il servizio, eventualmente condiviso da più organizzazioni, sia efficace anche al verificarsi contemporaneo di più eventi disastrosi).

3.5 VINCOLI E REQUISITI

I vincoli che caratterizzano la fornitura del servizio sono essenzialmente:

- tempi e modalità di consegna della documentazione di analisi e pianificazione;
- tempi e modalità di consegna ed attivazione del servizio;
- dislocazione dei sistemi e/o delle infrastrutture che realizzano la soluzione di continuità operativa (in particolare, distanza dal centro elaborazione dati principale);
- modalità di disponibilità del centro di elaborazione dati sul sito di ripristino (es. modalità condivisa, o modalità riservata);
- risorse disponibili (competenze specializzate, ambienti HW e SW disponibili);
- eventuali vincoli relativi a standard tecnici, documentali e normativi;
- finestra temporale di consegna e durata dell'erogazione del servizio.

I requisiti che caratterizzano la fornitura sono essenzialmente:

- estensione del perimetro informatico oggetto della continuità operativa;
- prestazioni richieste in termini di RTO ed RPO;
- livello di servizio che la piattaforma deve garantire in caso di gestione straordinaria;
- numero e tipologia dei Test periodici di Continuità Operativa;
- funzionalità ed efficienza richieste.

3.6 STANDARD E NORME APPLICABILI

Standard in materia di continuità operativa

Esistono standard emessi da enti nazionali, nordamericani ed europei, che sono spesso riconosciuti come riferimenti anche oltre i confini delle nazioni dove sono stati prodotti.

E' possibile citare:

- lo standard britannico BSI (British Standard Institute) PAS 56 "Guide to Business Continuity Management";
- lo standard americano NFPA 1600:2004 "Standard on Disaster/Emergency Management and Business Continuity Programs";
- lo standard prodotto dallo SPRING ("Standards, Productivity and Innovation Board"), una organizzazione di ispirazione governativa di Singapore SS507 "Singapore Standards for Business Continuity/Disaster Recovery (BC/DR) Service Providers".

Lo standard BSI PAS 56 sta per essere convertito in uno standard BSI di più alto livello (secondo la gerarchia BSI). Si tratta dello standard BS 25999 che sarà costituito da due parti, secondo il consueto schema "should/shall":

- BS 25999-1:2006 "Code of Practice for BCM", che costituisce l'evoluzione del PAS 56 (atteso per Novembre 2006);
- BS 25999-2:2006 "A Specification for BCM" (atteso nella prima metà del 2007).

Particolare è lo standard prodotto dallo SPRING, che si propone di dare indicazioni a organizzazioni nella scelta di un fornitore del servizio di Continuità Operativa.

Un discorso a parte deve essere fatto per alcuni standard ISO. Pur non esistendo ad oggi uno standard specifico per la Continuità Operativa, le norme ISO/IEC 17799:2005 "Information technology - Security techniques - Code of practice for information security management" e la recentissima ISO/IEC 27001 "Information technology — Security techniques — Information security management systems — Requirements", pur riguardando il processo di messa in sicurezza di un sistema informatico, anche dal punto di vista della certificazione, fanno riferimento a un sistema di Continuità Operativa quale requisito richiesto perché un sistema informatico sia considerato in sicurezza.

Sono disponibili alcuni framework di riferimento utilizzabili anche per la gestione della Continuità Operativa.

I principali sono:

- OGC (Office of Government Commerce) IT Infrastructure Library (ITIL v3).
Si vedano i libri "Business Continuity Management" e "Service Management" (sezione "Service Continuity Management").
ITIL è alla base degli standard BS15000 ed ISO/IEC 20000, dove si trovano ulteriori riferimenti alla Continuità Operativa; BS15000 ed ISO/IEC 20000 consentono un processo di certificazione più ampio e quindi inclusivo della Continuità Operativa.
- ITGI (IT Governance Institute) CobiT 4.0.
Vedasi il dominio DS4 "Ensure Continuous Service" ed i relativi 10 obiettivi di controllo.

I seguenti Istituti pubblicano guide di riferimento per la Continuità Operativa, e forniscono certificazioni specifiche:

- The Business Continuity Institute (www.thebci.org)
- Disaster Recovery International Institute (www.drii.org/DRII; materiale di riferimento è disponibile sul collegato Disaster Recovery's Journal: www.drj.com).

Norme in materia di continuità operativa

- Direttiva del Ministro per l'innovazione e le tecnologie
 - Il 16 gennaio 2002 il Ministro per l'innovazione e le tecnologie ha emanato una Direttiva in materia di "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali", pubblicata sulla G.U. n. 69 del 22 marzo 2002. Questa direttiva sollecita le pubbliche amministrazioni a porre attenzione ai temi della sicurezza, valutando i rischi e attuando contromisure in grado di contenerne probabilità e conseguenze.
- Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196).
 - Anche la normativa in materia di trattamento dei dati personali deve essere presa in considerazione nel disegnare soluzioni di continuità operativa: la legge infatti

mira a tutelare l'integrità, la disponibilità e la riservatezza dei dati, stabilendone le modalità di trattamento. I primi due aspetti (integrità e disponibilità) costituiscono l'obiettivo principale delle soluzioni di continuità operativa.

- Codice dell'amministrazione digitale (Decreto legislativo 7 marzo 2005, n. 82)
 - Il nuovo Codice dell'amministrazione digitale richiama indirettamente la necessità di salvaguardare i dati attinenti servizi pubblici. Il Codice richiede, tra l'altro, una particolare attenzione da parte delle amministrazioni alla custodia dei dati, in modo da garantire al meglio il diritto dei cittadini e delle imprese.
- D.P.C.M. 31 maggio 2005 (Gazz. Uff. 18 giugno 2005, n. 140)
 - L'art. 3, lettera c) di tale decreto, recante "Razionalizzazione in merito all'uso delle applicazioni informatiche e servizi ex articolo 1, commi 192, 193 e 194 della legge n. 311 del 2004 (Finanziaria 2005)", stabilisce che "Gli obiettivi di miglioramento dell'efficienza operativa della pubblica amministrazione e di contenimento della spesa pubblica sono conseguiti mediante interventi di razionalizzazione di infrastrutture di calcolo, telematiche e di comunicazioni delle amministrazioni" [...]. Gli interventi riguardano: [...] "c) centri per garantire la salvaguardia dei dati e delle applicazioni informatiche e la continuità operativa dei servizi informatici e telematici, anche in caso di disastri e di situazioni di emergenza, attraverso la definizione di infrastrutture, sistemi e servizi comuni a più amministrazioni, anche utilizzando CED già esistenti."
- Documento "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" del Comitato Tecnico Nazionale di sicurezza informatica del marzo 2004.
 - La seconda parte, "Linee guida per l'attuazione della sicurezza ICT nella PA", contiene l'indicazione di una serie di attività, che il Comitato ritiene di estrema urgenza, per l'analisi del rischio e la continuità operativa.
- Normativa generale per l'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 Direttiva 31 marzo 2004, n. 2004/18/CE, recante "Direttiva del Parlamento europeo e del Consiglio relativa al coordinamento delle procedure di aggiudicazione degli appalti pubblici di lavori, di forniture e di servizi";
 - il decreto legislativo D.Lgs. 12 aprile 2006, n. 163, recante "Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE".

3.7 RELAZIONI CON ALTRE CLASSI DI FORNITURA E MANUALI

La tabella seguente presenta un quadro di sintesi delle Classi di Fornitura che si stima principalmente essere in relazione con la presente.

Istanza / Fasi		Attività	Classe di Fornitura
Analisi e Pianificazione		Tutte	6.1.1 PGD Documentazione (Processo Trasversale)
		1.1 Risk assessment; 1.2 Business Impact Analysis; 1.3 Recoverability Assessment	4.1.1 CON Consulenza
		1.4 Disegno della Soluzione e del Servizio di CO	3.2.1SSI Sviluppo Sistemi
Erogazione del Servizio:	Implementazione	2.1 Realizzazione dell'infrastruttura; 2.2 Redazione del piano di continuità; 2.3 Configurazione ed attivazione; 2.5 Collaudo dell'infrastruttura	5.1.1 FPD Fornitura Prodotti Hardware e Software 2.1.2 ISI Integrazione di sistemi e infrastrutture
		2.2 Redazione del Piano di Continuità operativa (ICT)	4.1.1 CON Consulenza 6.1.1 PGD Documentazione (Processo Trasversale)
		2.4 Comunicazione / Formazione	1.3.2 FOR Formazione e addestramento
		Gestione e Manutenzione del Servizio	3.1 Esecuzione (primo) Test di continuità operativa; 3.4 Esecuzione Test periodici di continuità operativa
	3.2 Adeguamento Infrastruttura della Continuità Operativa		5.1.1 FPD Fornitura Prodotti Hardware e Software
	3.3 Aggiornamento del Piano di Continuità operativa (ICT); 3.5 Aggiornamento Sistema conoscenza Help Desk		4.1.1 CON Consulenza 6.1.1 PGD Documentazione (Processo Trasversale)
	Gestione e Manutenzione Straordinaria	4.1 Intervento in caso di crisi; 4.2 Gestione straordinaria	3.2.2 GSI Gestione sistemi 3.2.3 MSI Manutenzione sistemi
		4.3 Rientro	
		4.4 Aggiornamento del Piano di Continuità operativa (ICT)	4.1.1 CON Consulenza 6.1.1 PGD Documentazione (Processo Trasversale)

L'istanza di erogazione del servizio di continuità operativa suggerisce una strategia di acquisizione di tipo fornitura di servizi.
 Per questa modalità di acquisizione, si rimanda al Manuale Applicativo "Strategie di Acquisizione delle Forniture ICT"; la presente classe di fornitura fornisce informazioni specifiche sulla natura del servizio di continuità operativa, in particolare relativamente alle modalità di controllo e verifica della prestazione (vd. Manuale Applicativo "Strategie di Acquisizione delle Forniture ICT" - § 8.5, "Modalità di controllo e verifica della prestazione"; v. 1.0 del 25/01/2005).

4 MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA

Il problema della valutazione dei costi di un servizio di continuità operativa è alquanto complesso per l'elevato numero di fattori che entrano in gioco.

I costi dipendono, infatti, dalle caratteristiche della soluzione di continuità operativa, che possono essere espresse con più parametri:

- RTO (tempo di ripartenza);
- RPO (massimo scostamento temporale dell'allineamento dei dati tra il sito primario ed il sito di recovery);
- versatilità della soluzione (cioè possibilità di utilizzo anche in condizioni di gestione ordinaria del servizio);
- qualità e sicurezza dei servizi in condizioni di emergenza;
- probabilità di recupero (ossia probabilità che la soluzione, eventualmente condivisa da più organizzazioni, sia efficace anche al verificarsi contemporaneo di più eventi disastrosi);
- tempo massimo di permanenza in condizioni di emergenza.

Queste variabili sono tra di loro indipendenti e, anche se alcune combinazioni non sono significative, è teoricamente possibile "costruire" la soluzione scegliendo il valore più opportuno per ciascun parametro.

Nel seguito è fornita una breve descrizione di come i principali elementi di costo vengano influenzati dai parametri della soluzione.

Costo relativo alla fase di Analisi e Pianificazione

Il costo relativo alla fase di analisi è funzione della complessità dell'amministrazione ed è invariante rispetto ai parametri espressi.

La predisposizione del piano richiede risorse professionali variabili tra 10 giorni persona, per organizzazioni molto semplici, fino a qualche anno persona per amministrazioni particolarmente complesse.

In prima approssimazione si può ipotizzare che tale costo sia proporzionale alla complessità dell'amministrazione ed al numero dei dipendenti.

Costi d'impianto

I costi d'impianto sono relativi principalmente alla predisposizione del sistema alternativo per il ripristino. I costi sono dovuti ai prodotti informatici aggiuntivi (sistemi, apparati di rete, software) e, in maggiore misura, alle infrastrutture logistiche ed ai servizi presso il sito alternativo.

La spesa per il sistema alternativo incide sul tempo di ripartenza, la versatilità della soluzione, la qualità e sicurezza dei servizi in condizioni di emergenza, la probabilità di recupero ed il tempo massimo di permanenza in condizioni di emergenza.

Il costo dipende dai seguenti fattori:

- i parametri di qualità citati;
- la complessità e la dimensione del sistema alternativo;
- il livello di condivisione con altre organizzazioni.

In prima approssimazione, trascurando alcuni parametri che incidono sui costi in modo meno significativo, si può ipotizzare che tale voce di costo sia direttamente proporzionale alla spesa per il sistema informatico ed inversamente proporzionale al tempo di ripartenza ed al livello di condivisione del centro.

Allineamento dei dati

Al costo per l'allineamento dei dati concorrono principalmente le spese di trasporto dei nastri di backup o, in alternativa, i canoni per i servizi di trasmissione dati.

Questo costo assume un valore discontinuo a seconda della soluzione ed è in relazione con il massimo intervallo di transazioni perse (RPO), il numero di utenti serviti, il tempo di ripartenza e la probabilità di recupero .

Costi della Gestione e Manutenzione del Servizio

Questa voce di costo è dovuta alle seguenti attività continuative:

- manutenzione hardware del sistema alternativo
- aggiornamento software del sistema alternativo
- canoni e consumo per il sito alternativo
- gestione quotidiana del sito alternativo
- gestione periodica (prove)
- manutenzione e adeguamento delle soluzione

Questa spesa incide principalmente sulla qualità e sicurezza dei servizi in condizioni di recupero.

Tale costo può essere valutato come una percentuale dell'intero costo per la continuità operativa (10% - 30%).

Costi della Gestione Straordinaria

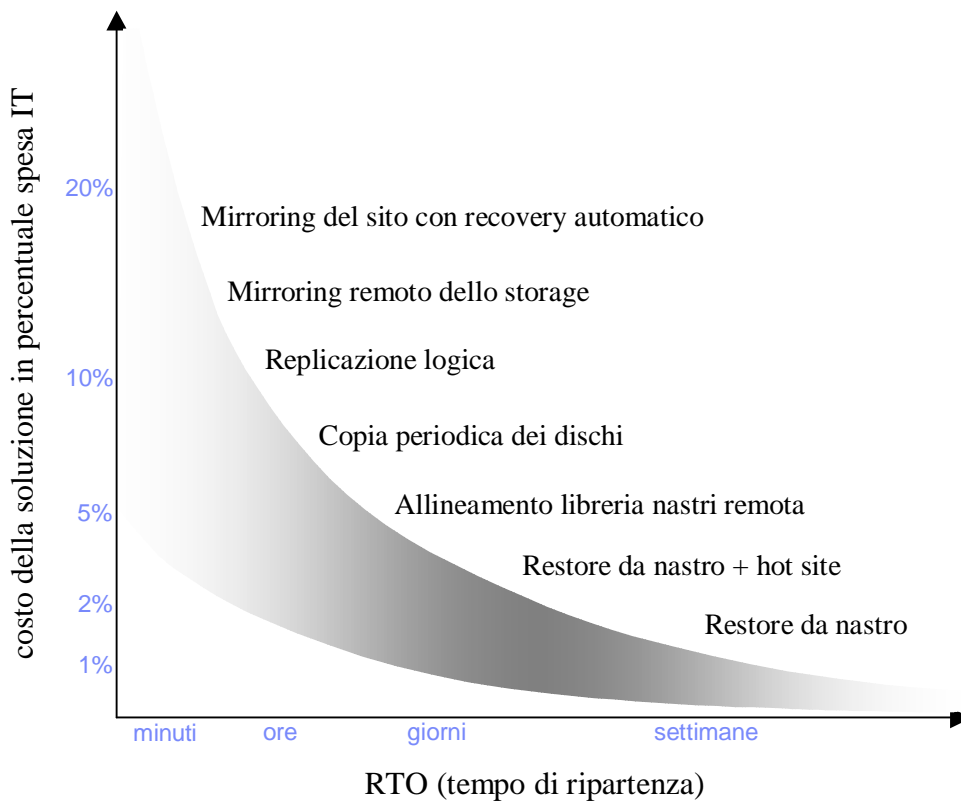
Oltre ai costi di gestione e manutenzione ordinaria del servizio, vi è il costo del servizio di gestione straordinaria, ovvero il costo della gestione del sistema informatico oggetto della continuità operativa presso il sito di recovery, a valle del verificarsi di un evento disastroso.

L'amministrazione avrà cura di indicare tra i requisiti un periodo temporale massimo di utilizzo del sito di recovery, trascorso il quale essa si impegna a ritornare alle condizioni di utilizzo originarie del sito stesso.

Relazione tra costo e tempo di ripartenza

Per semplificare il tema della stima dei costi, è possibile considerare, tra tutti, il parametro relativo al tempo di ripartenza (RTO). Secondo questo approccio le soluzioni sono definite a partire da questo requisito assumendo, in prima approssimazione, che gli altri parametri siano correlati al tempo di ripartenza: a valori ridotti di RTO corrisponderanno buoni indicatori per gli altri parametri mentre, di converso, se si accettano tempi lunghi di ripartenza, è probabile che si accettino anche caratteristiche minimali per gli altri fattori.

Con questa assunzione, le soluzioni vengono rapportate al requisito "tempo di ripartenza" ed i costi risultano inversamente proporzionali al valore assunto da tale parametro, come mostrato nella figura seguente.



Nella figura si è voluto comunque evidenziare come il solo parametro RTO non consenta di determinare univocamente il costo della soluzione ma, a parità di tempo di ripartenza, i costi possano variare all'interno di una fascia in funzione degli altri elementi caratterizzanti la soluzione. Ad esempio, tutte le soluzioni che prevedono un sito di backup hanno un costo variabile in funzione del livello di condivisione di tale sito con altre organizzazioni.

5 DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI

Le attività ed i prodotti relativi ai processi organizzativi e di supporto (processi trasversali), e cioè per esempio quelli relativi a gestione, documentazione, gestione della configurazione e assicurazione della qualità non sono descritti in questa scheda. Per la loro descrizione si rimanda pertanto alle schede specifiche.

Nel caso in cui attività o prodotti relativi a questi processi abbiano particolare rilevanza o criticità per la classe, essi sono comunque richiamati, evidenziando gli aspetti rilevanti o critici, rimandando per le caratteristiche generali alla scheda del processo.

5.1 QUADRO COMPLESSIVO

Il diagramma di flusso seguente illustra le due istanze di cui si compone la Classe di Fornitura e le macro relazioni tra macro attività e prodotti principali. Lo schema illustra anche i gruppi organizzativi cui affidare le varie attività: la nomenclatura di questi gruppi deve intendersi

puramente indicativa, mentre ruoli e responsabilità sono conformi a quanto delineato nelle Linee Guida.

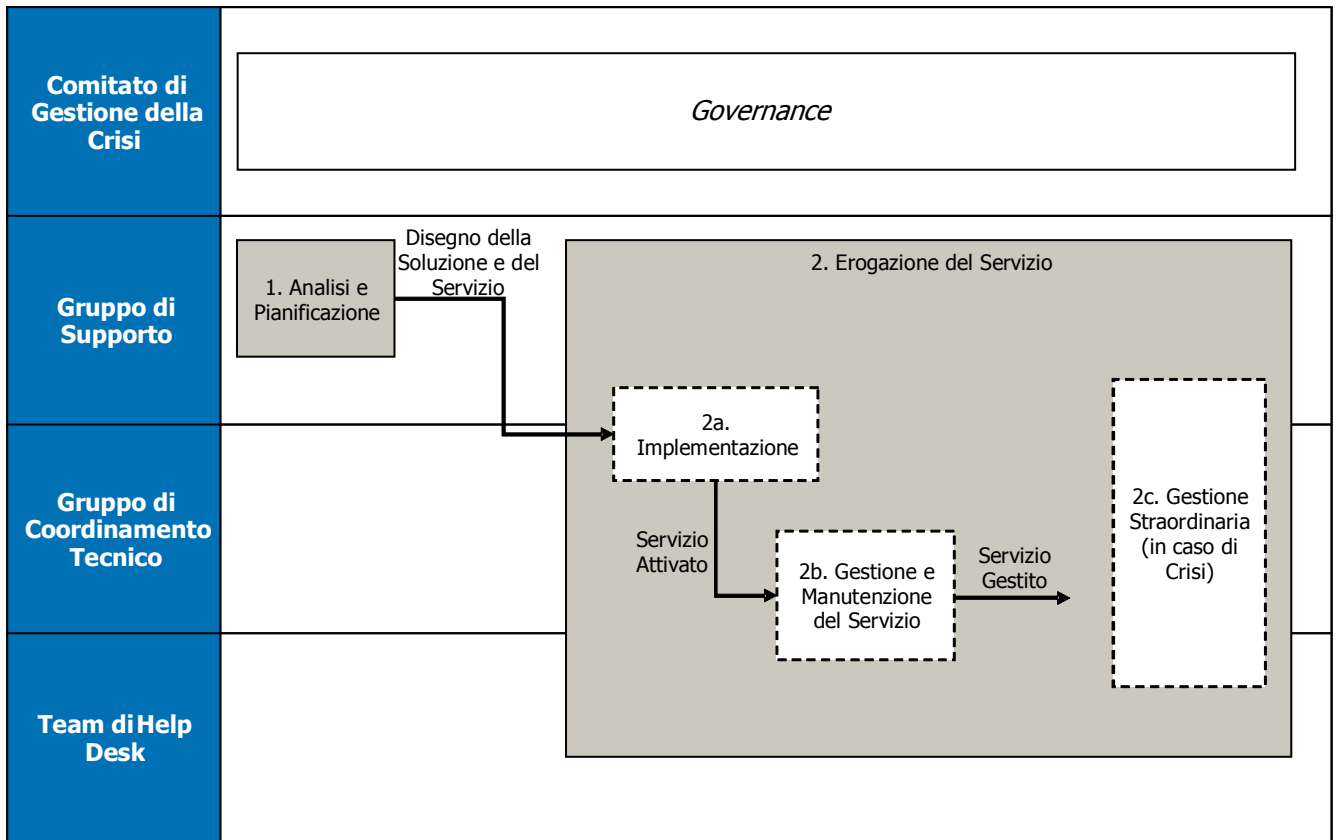


Diagramma 0 – Quadro generale del servizio di Continuità Operativa

La tabella seguente fornisce indicazioni schematiche sull'organizzazione per la gestione della Continuità Operativa. Per ulteriori dettagli si rimanda alle "Linee Guida alla Continuità Operativa nella Pubblica Amministrazione" (Par. 3.4).

Organizzazione	Responsabilità
Comitato di Gestione della Crisi	<p><u>Gestione ordinaria:</u> è il responsabile del processo di continuità operativa. Approva il piano di continuità; valuta periodicamente (annualmente) il livello di maturità della continuità operativa e promuove il miglioramento continuo.</p> <p><u>Gestione straordinaria (in emergenza):</u> assume il controllo di tutte le operazioni ed assume le responsabilità sulle decisioni per affrontare l'emergenza. valuta le situazioni di emergenza e dichiara lo stato di crisi, rapporti esterni/interni, attiva il processo di rientro, gestisce i conflitti.</p>
Gruppo di Supporto	<p><u>Gestione ordinaria:</u> responsabile della redazione del piano di continuità operativa, della sua gestione e manutenzione; dell'adeguamento periodico del BIA (Business Impact Analysis; studi, scenari finalizzati alla continuità operativa; rapporti con le assicurazioni, sensibilizzazione.</p> <p><u>Gestione straordinaria:</u> responsabile coordinamento gestionale delle attività e di relazione al Comitato della Sicurezza ICT (Direttiva DIT 16/01/2002)</p>

<p>Gruppo di Coordinamento Tecnico</p>	<p><u>Gestione ordinaria:</u> responsabile di tutte le attività operative e tecniche connesse con l'esecuzione delle procedure di recupero e rientro, ovvero esercitazioni e test periodici e manutenzione dell'infrastruttura tecnologica ed applicativa di recupero.</p> <p><u>Gestione straordinaria:</u> responsabile del coordinamento del personale operativo in emergenza e rapporti con terzi in ambito ICT (es. outsourcing), aspetti di logistica, relazione al Comitato di Gestione della Crisi.</p>
<p>Team di Help Desk</p>	<p><u>Gestione ordinaria:</u> aggiornamento dei sistemi di gestione della conoscenza a supporto degli operatori del normale help desk; predisposizione di canali alternativi al normale help desk da adottare in caso di emergenza.</p> <p><u>Gestione straordinaria:</u> rafforzamento help desk di primo livello; fornitura informazioni sullo stato dei sistemi periferici al Gruppo di Coordinamento Tecnico.</p>

Per ciascuna attività viene data la stima indicativa dell'effort, fatto 100 il totale delle attività di ogni singola fase (Analisi e Pianificazione, Implementazione, Gestione e Manutenzione del Servizio, Gestione e Manutenzione Straordinaria).

Si è ipotizzato che l'Amministrazione ed il suo sistema informativo sia di complessità e dimensioni medio-grandi, il tempo di ripartenza sia nell'ordine delle ore, il centro sia condiviso con altre Amministrazioni/clienti del Fornitore, la durata massima della gestione straordinaria sia nell'ordine di alcuni giorni.

Si è ipotizzato inoltre che la fase di Gestione e Manutenzione del Servizio, in cui sono presenti attività sia ripetitive che prevalentemente legate all'avvio del servizio, abbia durata di 1 anno.

Nei paragrafi successivi si entrerà in maggior dettaglio rispetto a quanto descritto nel precedente quadro complessivo. Ogni macro attività sarà a sua volta scomposta in attività particolari, ad ognuna delle quali sarà dedicata una trattazione specifica. Inoltre, nell'introduzione di ogni paragrafo, ognuna di queste attività sarà rappresentata in una tabella riepilogativa nella quale sono specificati:

- una stima indicativa del peso percentuale di effort richiesto;
- i prodotti di input e di output;
- i profili professionali EUCIP responsabili dell'esecuzione dell'attività.

5.2 ANALISI E PIANIFICAZIONE PER LA CONTINUITÀ OPERATIVA

Il prodotto complessivo di questa istanza costituisce uno strumento decisionale per l'Amministrazione rispetto alla soluzione di continuità da adottare ed anche uno strumento a supporto della stesura del capitolato, in quanto contenente tutti gli elementi essenziali per la definizione dell'approvvigionamento dei prodotti / servizi di realizzazione.

Le attività attinenti la realizzazione di questa fase per la continuità operativa sono riportati nella seguente tabella:

ATTIVITA'	% EFFORT	INPUT	OUTPUT	PROFILI PROFESSIONALI RESPONSABILI
1.1 Risk Assessment	25%		Relazione di valutazione del rischio (Risk Assessment)	Revisore di Sistemi Informativi
1.2 Business Impact Analysis	20%	Risk Assessment	Relazione di analisi di impatto per l'amministrazione (BIA - Business Impact Analysis)	Revisore di Sistemi Informativi
1.3 Recoverability Assessment	20%		Relazione di valutazione continuità corrente (RA - Recoverability Assessment)	Revisore di Sistemi Informativi
1.4 Disegno della Soluzione e del servizio di Continuità Operativa	35%	Business Impact Analysis Gap Analysis	Disegno del servizio di Continuità Operativa, contenente almeno: <ul style="list-style-type: none"> ○ situazione corrente; ○ architettura tecnologica ed operativa della soluzione di continuità operativa ○ requisiti (obiettivi di ripristino) e livelli di servizio; ○ organizzazione dell'amministrazione (area ICT) ○ piano esecutivo; ○ piano formativo. 	Consulente per la Sicurezza
Totale Analisi e Pianificazione per la Continuità Operativa	100%			

Ogni amministrazione potrà optare per uno dei due approcci possibili: un approccio basato sulle procedure amministrative tale da delimitare il campo di analisi alle risorse del sistema informatico che supportano le procedure di maggiore impatto sulla continuità operativa; oppure, un approccio basato sulle risorse del sistema informatico che appaiono ad elevato profilo di rischio tale da circoscrivere l'analisi alle procedure amministrative supportate dalle risorse con tale profilo di rischio.

Sulla relazione tra le attività di BIA e di Risk assessment si faccia riferimento al documento "Linee Guida alla Continuità Operativa nella Pubblica Amministrazione" (vd. Par. 1.1.2).

Il diagramma seguente illustra in modo grafico il flusso delle attività. Come si vedrà in dettaglio nel seguito, l'attività di recoverability assessment è maggiormente indicata laddove l'amministrazione abbia già in essere soluzioni di continuità operativa (evidentemente, da aggiornare o adeguare ad avvenuti cambiamenti).

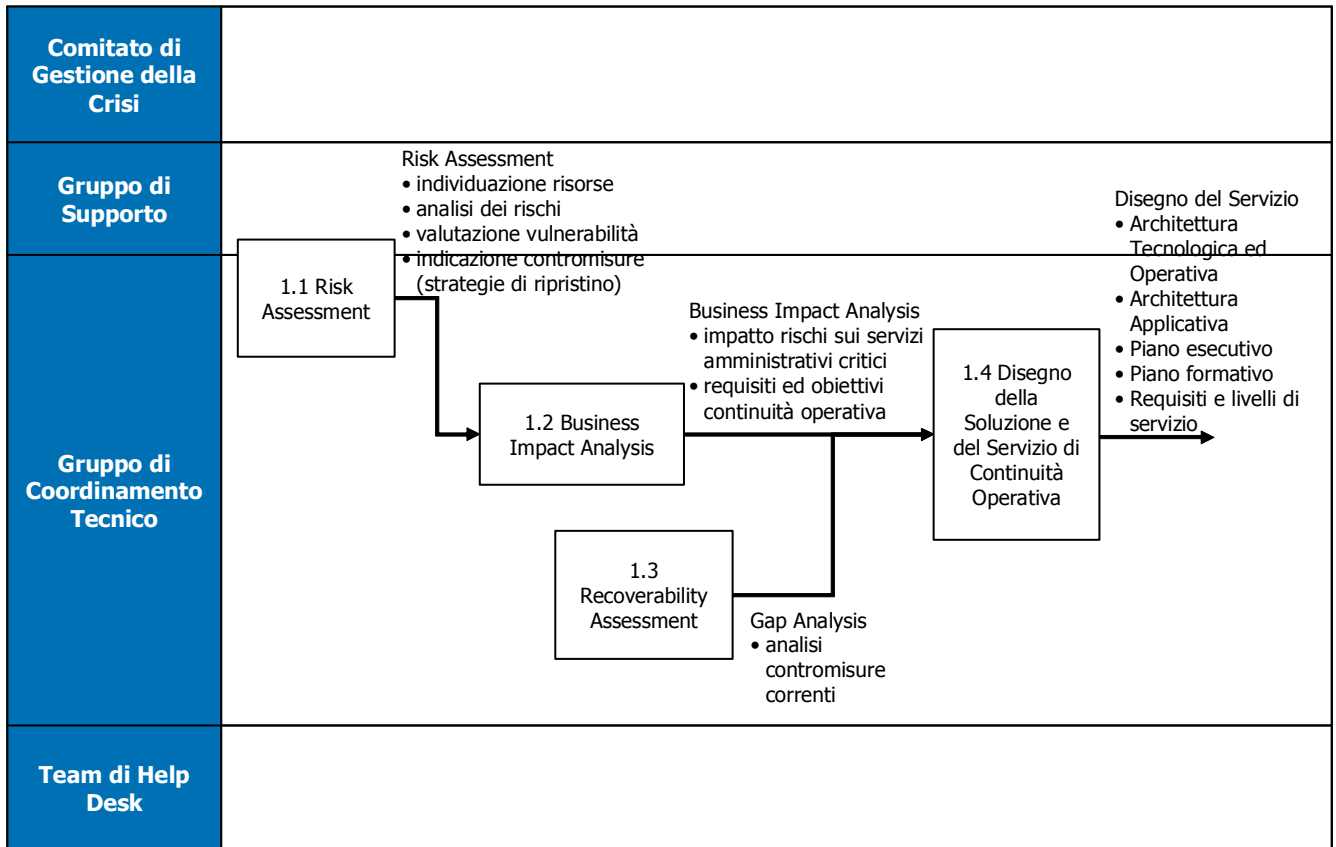


Diagramma 1 – Analisi e Pianificazione

Risk Assessment (1.1)

In questa fase vanno determinati, analizzati e classificati i rischi a cui è soggetta l'amministrazione, e vanno stimate le vulnerabilità dell'amministrazione, in modo che quest'ultima sia poi capace di valutare le salvaguardie più adeguate ed efficaci.

L'attività richiede i seguenti passi, da realizzarsi attraverso la raccolta della documentazione esistente e/o attraverso la richiesta di informazioni (incontri, interviste, questionari) al personale amministrativo e/o tecnico competente:

- identificazione dei beni informatici dell'amministrazione che necessitano protezione;
- classificazione dei beni in termini di esigenza di disponibilità (continuità operativa), sia ai fini della corretta erogazione dei servizio, sia, più in generale, della sicurezza e della tutela del patrimonio pubblico;
- valutazione (in genere qualitativa o semi-quantitativa) della vulnerabilità dei beni rispetto alle varie minacce possibili;
- classificazione delle minacce, in termini di probabilità di accadimento (frequenza) e di danno economico potenziale.

La "Relazione di valutazione del rischio" (documento di Risk Assessment), deve contenere quindi le seguenti informazioni:

- Ambito (beni informatici);

- Analisi della vulnerabilità dei beni in ambito rispetto alle minacce (eventi disastrosi) e classificazione delle minacce;
- Determinazione del livello di rischio corrente e del livello di rischio accettabile;
- Determinazione delle priorità di intervento;

Business Impact Analysis (1.2)

Questa attività (il termine inglese è traducibile con “valutazione dell’impatto sull’operatività”) ha lo scopo di determinare le conseguenze derivanti dal verificarsi di un evento critico e di valutare l’impatto di tale evento sull’operatività dell’amministrazione.

Lo svolgimento di una BIA prevede i tre passi descritti nel seguito.

- individuazione delle procedure amministrative e dei servizi critici (l’amministrazione definisce il livello di profondità dell’analisi nella struttura delle procedure amministrative)
- identificazione dell’insieme delle risorse informatiche (incluso il personale) a supporto delle procedure e dei servizi critici
- analisi dell’impatto dell’indisponibilità prolungata (e relativa individuazione degli obiettivi di ripristino)
- determinazione delle strategie di ripristino opportune.

Gli obiettivi di ripristino sono individuati dai seguenti parametri:

- RTO (Recovery Time Objective): per quanto tempo l'amministrazione può sopportare l'interruzione o il degrado prestazionale della procedura o servizio resosi indisponibile a fronte di un evento;
- RPO (Recovery Point Objective): in quale misura l'amministrazione può sopportare la perdita di dati associati alla procedura o servizio in esame.

La Relazione di analisi di impatto per l’amministrazione (Business Impact Analysis), contiene quindi le seguenti informazioni minime:

- Identificazione delle esigenze generali di continuità operativa
- Approccio adottato
- Caratterizzazione delle procedure e servizi dell'amministrazione
- Caratterizzazione dei sistemi informatici
- Identificazione delle esigenze di continuità operativa dei sistemi informatici (obiettivi RTO, RPO)
- Priorità di intervento

Recoverability Assessment (1.3)

Il recoverability assessment (traducibile in italiano con “verifica della capacità di mantenimento della continuità”) ha lo scopo di valutare l’attuale capacità dell’amministrazione di supportare gli obiettivi di continuità prefissati mediante le procedure, l’organizzazione e le risorse informatiche correnti. In altre parole, durante questa fase si vuole valutare la distanza (definita anche “*gap*”) tra la situazione attuale e quella ottimale.

La Relazione di recoverability assessment si applica quindi alle risorse del sistema informatico a supporto di procedure amministrative per le quali sono correntemente adottate soluzioni di continuità operativa e contiene quindi le seguenti informazioni minime:

- caratterizzazione delle risorse informatiche nell'ambito della soluzione di continuità corrente;
- caratterizzazione della capacità di protezione dei dati (es. backup, restore, meccanismi di replica) e modalità di conservazione delle copie;
- stima degli obiettivi di ripristino della soluzione corrente;
- valutazione di distanza della soluzione di continuità operativa corrente rispetto agli obiettivi individuati dall'attività di BIA.

Disegno della Soluzione e del servizio di Continuità Operativa (1.4)

L'attività di disegno della soluzione e del servizio ha come obiettivo ultimo quello di delineare obiettivi, ambiti e caratteristiche del servizio di Continuità Operativa adeguato per l'amministrazione, attraverso la redazione di un documento tecnico che contiene almeno le seguenti informazioni:

- situazione corrente (architettura tecnologica ed operativa);
- architettura tecnologica ed operativa della soluzione di continuità operativa;
- requisiti (obiettivi di ripristino) e livelli di servizio;
- organizzazione e procedure IT dell'amministrazione nella gestione ordinaria e straordinaria;
- piano esecutivo (include le fasi di implementazione, gestione e manutenzione del servizio e straordinaria);
- piano formativo.

Questo documento tecnico in particolare realizza lo strumento di supporto nella stesura del capitolato relativo all'istanza di erogazione del servizio nella presente classe di fornitura.

Il disegno della soluzione e del servizio di continuità operativa dovrà curare e fornire i requisiti relativi agli aspetti logistici.

5.3 EROGAZIONE DEL SERVIZIO: IMPLEMENTAZIONE

Come si è detto, al fine di facilitare la descrizione dell'istanza di Erogazione del Servizio, questa è suddivisa in tre fasi principali:

- Fase di Implementazione
- Fase di Gestione e Manutenzione del Servizio
- Fase di Gestione e Manutenzione Straordinaria

La fase di Implementazione prevede i seguenti obiettivi:

- realizzare la soluzione di continuità individuata, attraverso la acquisizione dei beni e la predisposizione delle strutture, delle tecnologie e dei meccanismi di copia dei dati e di automazione (secondo i livelli definiti opportuni dall'amministrazione) della procedura di intervento;

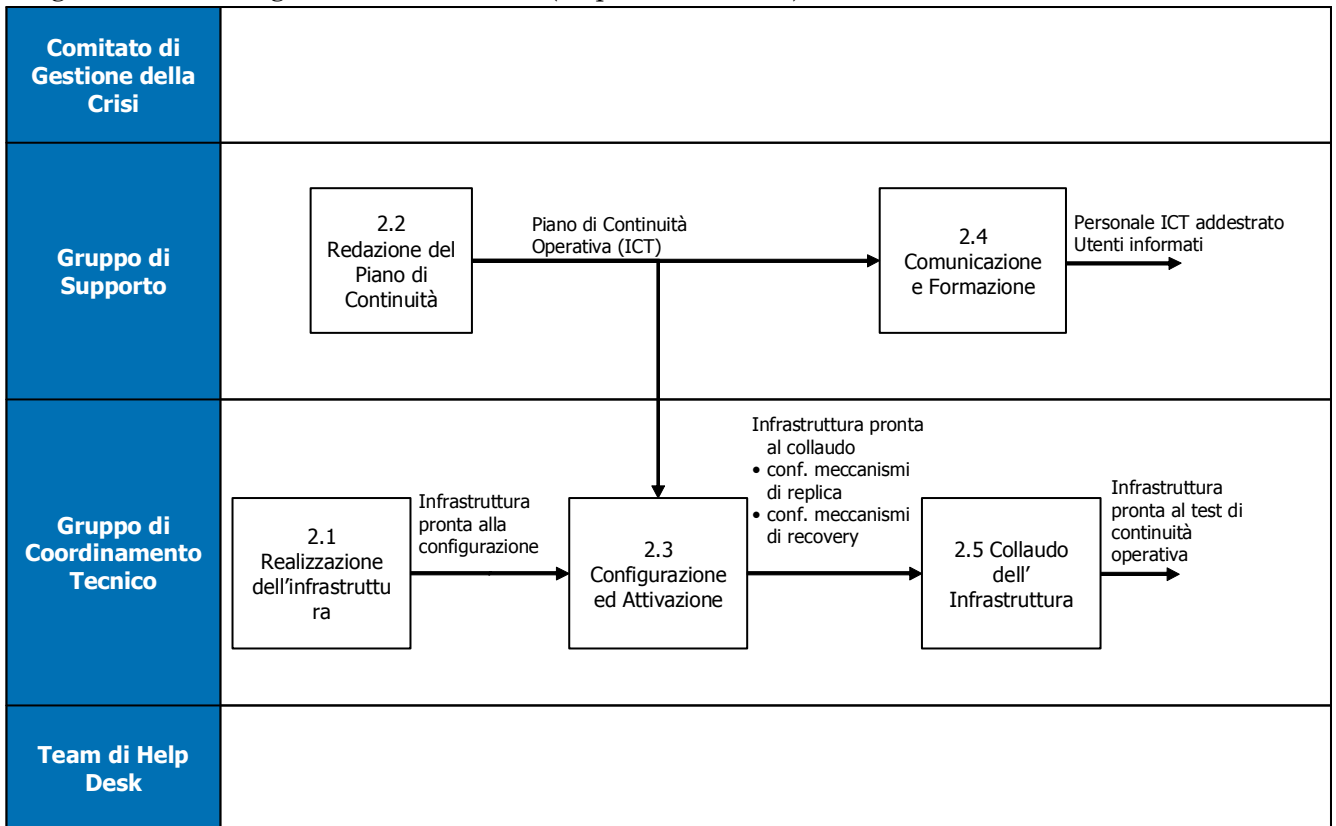
- eseguire il piano di comunicazione e formazione;
- formalizzare, all'interno di un documento denominato "Piano di continuità operativa", le procedure operative da adottare con esplicitazione dei ruoli e delle responsabilità, negli scenari di crisi considerati (cioè indirizzati in fase di Risk assessment);
- redigere il piano di collaudo dell'infrastruttura
- collaudare le funzionalità realizzate.

Che saranno realizzati attraverso le attività riportate in tabella.

ATTIVITA'	% EFFORT	INPUT	OUTPUT	PROFILI PROFESSIONALI RESPONSABILI
2.1 Realizzazione dell'Infrastruttura	30%	Architettura tecnologica ed operativa della soluzione di continuità operativa	infrastruttura pronta alla configurazione	Responsabile della Configurazione e del Centro Dati
2.2 Redazione del Piano di Continuità	30%	Risk assessment Requisiti (obiettivi di ripristino) e livelli di servizio	Piano di continuità	Consulente per la Sicurezza
2.3 Configurazione ed Attivazione	15%	Piano esecutivo	Infrastruttura pronta al collaudo	Responsabile della Configurazione e del Centro Dati
2.4 Comunicazione/ Formazione	15%	Piano di comunicazione Piano formativo Piano di Continuità	Personale ICT addestrato Utenti informati	Consulente per la Sicurezza
2.5 Collaudo dell'Infrastruttura	10%	Piano dei test Piano di collaudo	Infrastruttura pronta al test di continuità operativa	Tecnico di Collaudo e Integrazione di Sistemi
Totale Implementazione	100%			

Il diagramma di flusso seguente illustra le attività che costituiscono la fase di implementazione.

Diagramma 2 – Erogazione del Servizio (Implementazione)



Segue una descrizione di dettaglio delle singole attività.

Realizzazione dell'infrastruttura (2.1)

In questa fase si svolgono le attività pianificate nella istanza precedente, con riferimento alla realizzazione della infrastruttura tecnologica per la continuità.

Le problematiche affrontate dal fornitore in questa fase sono legate soprattutto alla gestione delle acquisizioni, agli aspetti finanziari delle stesse, alla tempistica delle consegne (ad esempio occorre curare che la consegna di apparecchiature avvenga a valle della disponibilità dei locali che dovranno ospitarle). L'amministrazione è coinvolta in questa fase nel caso in cui acquisti essa stessa i beni informatici e nei casi di adeguamento dell'infrastruttura del sito primario.

In generale, per uno svolgimento efficace di questa fase, l'indicazione è seguire le regole e le *best practice* valide nelle usuali attività di realizzazione di infrastrutture informatiche, non esistendo specificità particolari legate al tema della continuità operativa.

L'amministrazione ha la possibilità di acquisire in proprio (in tutto od in parte) le apparecchiature e gli strumenti necessari per l'erogazione del servizio di continuità operativa, oppure di richiedere al fornitore del servizio l'acquisizione di quanto necessario alla erogazione

del servizio stesso. In quest'ultimo caso, l'amministrazione fornirà al fornitore i requisiti per l'acquisizione dei componenti hardware e software, attraverso la descrizione dettagliata delle configurazioni e dei disegni architettonici dei componenti che costituiscono il sistema informatico corrente.

Il prodotto di questa attività è l'infrastruttura pronta alla configurazione di continuità. E' possibile prevedere un collaudo di conformità della fornitura e delle attività di installazione di base.

L'attività include la redazione del piano di collaudo dell'infrastruttura.

Redazione del Piano di Continuità (2.2)

Obiettivo di questa attività è formalizzare le procedure operative da adottare con esplicitazione dei ruoli e delle responsabilità, negli scenari di crisi considerati (cioè indirizzati in fase di Risk assessment).

Il Piano di continuità operativa è in questa sede riferito ai sistemi informatici: esso guida la direzione Sistemi Informativi nella gestione e mediazione dei rischi cui essa è soggetta. Il piano definisce ed elenca le azioni da intraprendere prima, durante e dopo una condizione d'emergenza per assicurare la continuità del servizio.

Il principale obiettivo del Piano è massimizzare l'efficacia delle operazioni in risposta a un'emergenza. Per ottenere questo risultato è necessario pianificare gli interventi previsti in modo ben definito, prendendo in considerazione le singole fasi in cui sono generalmente raggruppate le azioni da intraprendere in seguito al verificarsi dell'emergenza.

Esse sono:

- notifica al Comitato di Gestione della Crisi ai fini della valutazione del danno, e della dichiarazione di emergenza con la conseguente attivazione delle risorse destinate al ripristino;
- ripristino delle procedure e dei servizi attraverso le misure di disponibilità alternativa oggetto della fase di implementazione;
- in caso di interruzione prolungata, attivazione delle procedure per far fronte a un'indisponibilità prolungata nel tempo delle risorse necessarie all'erogazione dei servizi;
- gestione dell'operatività in condizioni ordinarie e straordinarie;
- ritorno alla normale operatività, cioè alle condizioni precedenti al verificarsi dell'emergenza.

Il Piano fornisce indicazioni anche su:

- pianificazione delle attività (trasversali alle fasi testé definite) di coordinamento con eventuali strutture esterne che concorrono all'erogazione dei servizi, compresi eventuali fornitori;
- assegnazione di ruoli e responsabilità, con particolare riferimento alla gestione straordinaria;
- documentazione di tutti gli aspetti tecnici che consentono di eseguire le operazioni di gestione dell'emergenza.

Un esempio di struttura del Piano della Continuità è il seguente:

- Sezione introduttiva

- Valutazioni BIA
- Valutazioni Risk Assessment
- Strategie di ripristino selezionate
- Quadro operativo
- Fase di notifica e attivazione
 - Procedure di notifica e attivazione
 - Valutazione del danno
- Fase di ripristino
 - Sequenza delle azioni di ripristino
 - Procedure di ripristino
- Fase di rientro alla condizione iniziale
- Appendici
 - Business Impact Analysis
 - Risk Assessment
 - Sistema informatico nel perimetro del Piano
 - Strategie di ripristino
 - Risultati delle simulazioni

Configurazione ed attivazione (2.3)

In questa fase dovranno svolgersi le attività relative alla messa in opera dei meccanismi di protezione dei dati e di configurazione della componente tecnologica della soluzione di continuità.

Le problematiche da affrontare in questa fase sono legate al tipo di soluzione tecnologica ed alle strategie di ripristino selezionate. In generale, saranno approntati i meccanismi di copia dei dati ed eventualmente di automazione della procedura di intervento in emergenza.

Comunicazione / Formazione (2.4)

L'attività consiste nella esecuzione del piano di comunicazione e formazione, conformemente a quanto stabilito nell'attività di disegno della soluzione e del servizio di continuità operativa (istanza Analisi e Pianificazione).

Il piano di comunicazione è rivolto agli utenti (interni ed esterni) dell'amministrazione, con lo scopo di trasmettere le informazioni necessarie a tutti gli attori coinvolti nei possibili scenari d'emergenza.

La pianificazione della comunicazione e della formazione dovrà tenere conto della disponibilità di adeguati spazi (aule, sale riunioni, ecc.) e soprattutto della disponibilità del personale, da coinvolgere minimizzando l'impatto sulla normale operatività dell'amministrazione.

Per il personale tecnico incaricato della gestione delle componenti tecnologiche della soluzione di continuità (es. sistemi di storage, sito alternativo) dovrà essere pianificato un programma di formazione, finalizzato ad acquisire (o a completare l'acquisizione) le competenze necessarie all'esercizio della soluzione di continuità.

Com'è noto, esistono numerose modalità di addestramento possibili (training the trainer, affiancamento, in aula, corsi on line, ecc.): l'amministrazione dovrà scegliere quale modalità è la più adeguata alle proprie esigenze, tenendo anche in questo caso in massima considerazione l'esigenza di limitare l'impatto sulla normale operatività.

Collaudo dell'infrastruttura (2.5)

L'attività di collaudo dell'infrastruttura ha l'obiettivo di verificare che la soluzione tecnico-organizzativa posta in essere sia conforme al disegno ed ai requisiti di continuità, ovvero che sia adeguata al raggiungimento degli obiettivi di continuità definiti dall'amministrazione.

Nella fase di esecuzione dei test vengono attuate le verifiche e gli interventi pianificati in fase di definizione del piano dei test, secondo le modalità, l'approccio e la tempistica stabilite. Il collaudo dell'infrastruttura è relativo almeno ai seguenti ambiti:

- Test dei meccanismi di replica dei dati
- Test di conformità (accessi fisici, connettività) del/i sito/i alternativo/i
- Test delle soluzioni di protezione dei dati (snapshot, backup, vaulting, ecc.)
- Test della documentazione (verifica di completezza e correttezza degli aspetti documentali della soluzione di continuità, ed in particolare del Piano della Continuità).
- Test dei singoli componenti infrastrutturali oggetto di implementazione.

5.4 EROGAZIONE DEL SERVIZIO: GESTIONE E MANUTENZIONE DEL SERVIZIO

Le attività di gestione e manutenzione del servizio sono condotte generalmente su base periodica, in stretta relazione con le attività di gestione del cambiamento in area ICT. La periodicità di tali interventi è specifica di ogni singola amministrazione in funzione della criticità delle procedure, e della natura e della frequenza dei cambiamenti sia a livello organizzativo sia a livello componenti ICT.

La fase di Gestione e manutenzione del servizio prevede i seguenti obiettivi

- garantire l'allineamento della soluzione di continuità rispetto all'evoluzione del sistema informatico e della struttura organizzativa dell'amministrazione;
- verifica del grado di preparazione complessivo (amministrazione e fornitore) nel rispondere e gestire situazioni di crisi, in accordo con quanto previsto dalla soluzione di continuità prescelta;
- verifica del livello di aggiornamento del Piano di continuità operativa in funzione dei cambiamenti ICT intercorsi;
- valutazione dell'adeguatezza del Piano di continuità operativa nel ripristino dell'operatività (simulazione di crisi);
- identificazione ed attuazione delle eventuali misure di adeguamento e/o miglioramento (interventi di tipo tecnologico, organizzativo, procedurale e/o formativo e di comunicazione).

Realizzati attraverso le attività riportate nella tabella seguente:

ATTIVITA'	% EFFORT	INPUT	OUTPUT	PROFILI PROFESSIONALI RESPONSABILI
3.1 Esecuzione (primo) Test di Continuità Operativa	20%	Piano di continuità	Relazione esisto test	Tecnico di Collaudo e Integrazione di Sistemi
3.2 Adeguamento infrastruttura della continuità Operativa	25%	Richiesta di adeguamento o aggiornamento	Infrastruttura aggiornata	Responsabile della Configurazione e del Centro Dati
3.3 Aggiornamento del Piano di Continuità	15%	Richiesta di adeguamento o aggiornamento	Piano di continuità	Consulente per la Sicurezza
3.4 Esecuzione Test Periodici di Continuità Operativa	25%	Piano di continuità	Rapporto esecuzione test	Tecnico di Collaudo e Integrazione di Sistemi
3.5 Aggiornamento del Sistema di Conoscenza HelpDesk	15%	Piano di continuità	Help desk aggiornato	Supervisore di un Centro di Assistenza
Totale Gestione e Manutenzione del Servizio	100%			

Il diagramma di flusso seguente illustra le attività che costituiscono la fase di gestione e manutenzione del servizio.

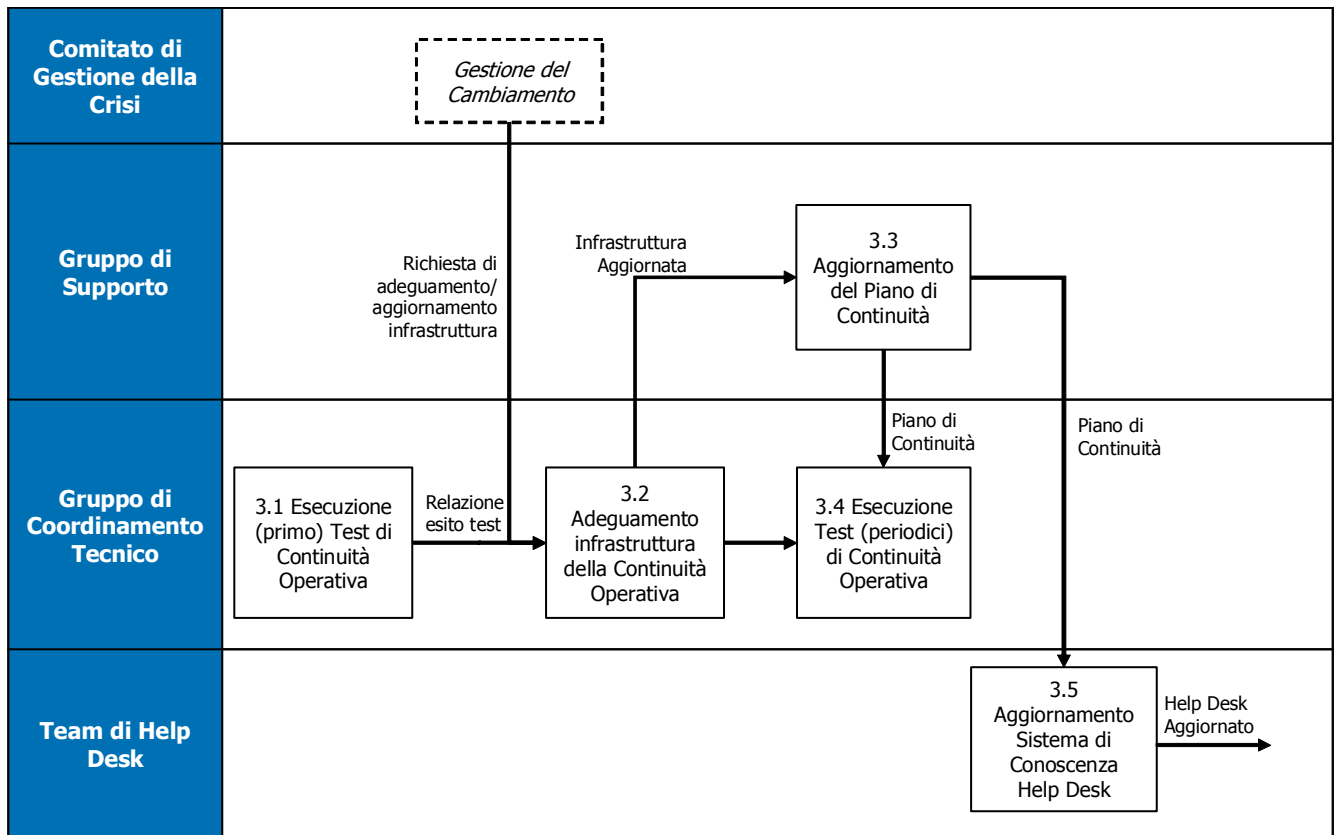


Diagramma 3 – Erogazione del Servizio (Gestione e Manutenzione del Servizio)

Segue una descrizione di dettaglio delle singole attività.

Esecuzione (primo) Test di Continuità Operativa (3.1) e Esecuzione Test Periodici di Continuità Operativa (3.1 e 3.4)

La responsabilità dell'esecuzione dei test di continuità operativa è dell'Amministrazione. Il Fornitore fornisce assistenza durante queste fasi, secondo quanto opportunamente concordato tra le parti.

Dopo il collaudo dell'infrastruttura, la soluzione è pronta al collaudo della continuità operativa; questo collaudo richiede la simulazione di un evento disastroso e la valutazione della capacità della soluzione proposta di garantire il livello di continuità operativa atteso, in termini tecnologici, organizzativi e procedurali.

Sono possibili numerose modalità di test che possono essere eseguiti anche contemporaneamente nel corso di un anno (ad es. quattro verifiche teoriche ed una simulazione all'anno) in funzione di esigenze specifiche di organizzazione e di cambiamento.

Si individuano quattro principali tipologie, elencate in ordine crescente di complessità:

- **Verifica teorica.** E' la metodologia più classica, e si riallaccia alle usuali tecniche di auditing e di validazione "su carta". Consiste nel condurre un'analisi di congruenza della soluzione, a cura degli autori stessi della soluzione o di esperti esterni.
- **Walk-through strutturato.** Si stabilisce uno scenario teorico di crisi, e i partecipanti al test percorrono ("walk-through") le attività previste dal Piano di Continuità operativa. Nel corso del walk-through si verificano e documentano eventuali errori o carenze.
- **Tattico.** Consiste in una simulazione condotta come "gioco di guerra". Tutte le persone coinvolte sono chiamati a eseguire le attività previste dal piano di continuità operativa, comunicate in anticipo o a sorpresa, sulla base delle informazioni rese note dal coordinatore della simulazione. La simulazione deve riproporre il più realisticamente possibile lo scenario di crisi ipotizzato.
- **Simulazione.** In questo caso il test coinvolge l'intero personale dell'amministrazione o almeno il personale addetto all'area interessata dalla simulazione. Il test prevede l'esecuzione "in tempo reale" del piano di continuità operativa e la verifica delle procedure, dei sistemi di backup, dei sistemi alternativi di comunicazione, della mobilitazione dei gruppi di gestione dell'emergenza, del recupero di documenti e dati. Condurre una simulazione di emergenza completa può avere un costo molto elevato; per questo in genere si usano simulazioni semplificate.

Quando sono previsti test periodici di simulazione, valgono i seguenti requisiti:

- le simulazioni devono essere progettate per simulare una "vera" condizione di emergenza, ricreando le conseguenze dell'evento peggiore nel peggior momento tra quelli valutati negli scenari di Risk Assessment (ad esempio, l'improvvisa indisponibilità del CED primario durante l'orario di punta dei servizi erogati);
- per non rischiare di compromettere i dati di produzione per l'effettuazione delle simulazioni, dovranno essere predisposte copie dei dati ad uso esclusivo della simulazione che saranno cancellate al termine delle prove;
- nel caso la soluzione preveda un centro alternativo, è necessario verificare e testare tutti quei processi e procedure che devono garantire, in condizioni di funzionamento normale del centro primario, le operazioni di allineamento dei due centri (copia remota dei dati, ecc.).

Adeguamento infrastruttura della Continuità Operativa (3.2)

La manutenzione del servizio della soluzione di continuità non è legata solo ai risultati dei test. E' necessario prevedere un processo di comunicazione formale tra fornitore ed amministrazione, che consenta a quest'ultima di esprimere una domanda di adeguamento del servizio di continuità operativa a seguito di interventi di *change management* sul sistema informatico primario; l'obiettivo ultimo è quello di mantenere aggiornato il servizio secondo le nuove situazioni che si vengono a creare, ad esempio, a seguito di:

- aggiunta di nuovi processi o servizi;
- variazioni delle configurazioni hardware o software;

- variazioni organizzative dell'amministrazione;
- nuovi requisiti di carattere legale o procedurale.

In presenza di sistemi informatici complessi, l'amministrazione potrà trovare utile dotarsi o chiedere al fornitore di dotarsi di soluzioni tecnologiche a supporto delle attività di gestione delle configurazioni (*configuration management*) tra i due siti (primario e di recovery) e di implementazione dei cambiamenti (*change management*).

A valle dell'esecuzione dei test di continuità operativa o a valle di una richiesta di adeguamento dell'infrastruttura (cambiamenti dovuti ad es. a nuovi progetti ICT), il Fornitore dovrà svolgere un'attività di implementazione dell'infrastruttura a supporto della continuità operativa.

Nel caso di adeguamenti dovuti a non conformità dei risultati del test con gli obiettivi di continuità attesi, si tratterà di adeguamenti correttivi.

Nel caso di adeguamenti dovuti in genere ai cambiamenti del sistema informatico o di sue parti, si tratterà di adeguamenti evolutivi.

Le attività da svolgere sono in genere equivalenti a quelle previste per la fase di Implementazione, ad esclusione della redazione del piano di continuità (che sarà aggiornato). Le attività di comunicazione e formazione sono quindi da includere.

Aggiornamento del Piano di Continuità (3.3)

Il Piano di Continuità viene aggiornato per riflettere i cambiamenti tecnologici, procedurali ed eventualmente organizzativi messi in campo per effetto dell'attività di adeguamento dell'infrastruttura.

L'aggiornamento del Piano di Continuità può comportare l'aggiornamento di risultati tipici della fase di Analisi (vedasi la struttura del Piano indicata nei precedenti paragrafi), quali il BIA, il Risk Assessment, la determinazione delle strategie di ripristino. Qualora il livello di aggiornamento sia significativo (ad es. per effetto della introduzione di nuovi procedimenti, e/o di nuove strategie di ripristino), può essere opportuno per l'amministrazione prevedere un contratto specifico di revisione dell'Analisi.

Si osservi che cambiamenti organizzativi nell'area ICT e procedurali amministrativi possono anch'essi determinare l'aggiornamento del Piano di Continuità.

E' cura dell'organizzazione ICT ed in particolare del Comitato di Gestione della Crisi avviare le richieste di cambiamento e/o approvare le attività di adeguamento a seguito dell'esito dei test periodici.

Aggiornamento del Sistema di Conoscenza Help Desk (3.5)

Nell'ambito della gestione e manutenzione del servizio, è cura del Fornitore definire un (o integrare nell'esistente) team di help desk specifico per la continuità operativa, i cui compiti sono:

- aggiornamento dei sistemi di gestione della conoscenza a supporto degli operatori del normale help desk (riguardo alle tematiche da affrontare in caso di emergenza);
- rafforzamento del normale help desk di primo livello in caso di emergenza;
- predisposizione di canali alternativi (al normale help desk) da adottare in caso di emergenza e diffusione presso gli utenti dei riferimenti relativi;

- fornitura di informazioni sullo stato dei sistemi in periferia al Gruppo di coordinamento tecnico;
- supporto agli utenti nelle difficoltà connesse alla ripresa delle attività al rientro.

Il team di help desk dovrà disporre di una copia aggiornata del Piano di Continuità.

Nella costituzione di tale team devono essere valutati specialmente la capacità di operare in assenza dei servizi informatici, la capacità di utilizzare canali multipli di comunicazione con gli utenti e la capacità di lavorare in situazione di emergenza.

5.5 EROGAZIONE DEL SERVIZIO: GESTIONE E MANUTENZIONE STRAORDINARIA

Le attività di gestione e manutenzione straordinaria sono quelle attività che, in conformità con quanto prescritto nel Piano della Continuità, devono essere realizzate per garantire la continuità del servizio in caso di crisi, ovvero di dichiarazione di un evento disastroso.

La fase di Gestione e manutenzione del servizio prevede i seguenti obiettivi (il cui dettaglio è definito nel Piano di Continuità):

- esecuzione delle procedure e delle azioni previste nel Piano di Continuità: intervento per il ripristino della continuità operativa (“Intervento”);
- gestione operativa straordinaria, ovvero gestione dei servizi informatici configurati per la continuità operativa, secondo i livelli di servizio pre-definiti in caso di crisi;
- esecuzione delle attività propedeutiche al rientro nelle condizioni di normalità.

Si osservi che la dichiarazione di crisi, la comunicazione di questa, il coordinamento, la richiesta di attivazione della soluzione di continuità operativa e la richiesta di rientro sono di reponsabilità e cura di esecuzione dell'Amministrazione.

Le attività previste sono ricapitolate nella seguente tabella:

ATTIVITA'	% EFFORT	INPUT	OUTPUT	PROFILI PROFESSIONALI RESPONSABILI
4.1 Intervento in caso di crisi	20%	Dichiarazione crisi (attivazione) Valutazione del danno	Sistema ripristinato Rapporto di intervento	Responsabile della Configurazione e del Centro Dati
4.2 Gestione straordinaria	40%	Rapporto di intervento Piano di Continuità Operativa	Sistema in modalità di emergenza Rapporto di Gestione Straordinaria	Responsabile della Configurazione e del Centro Dati
4.3 Rientro	25%	Piano di continuità	Sistema in modalità ordinaria Rapporto della crisi	Responsabile della Configurazione e del Centro Dati
4.4 Aggiornamento del Piano di Continuità	15%	Rapporto della crisi	Piano di continuità	Consulente per la Sicurezza
Totale Gestione e Manutenzione Straordinaria	100%			

Il diagramma di flusso seguente illustra le attività che costituiscono la fase di gestione e manutenzione straordinaria.

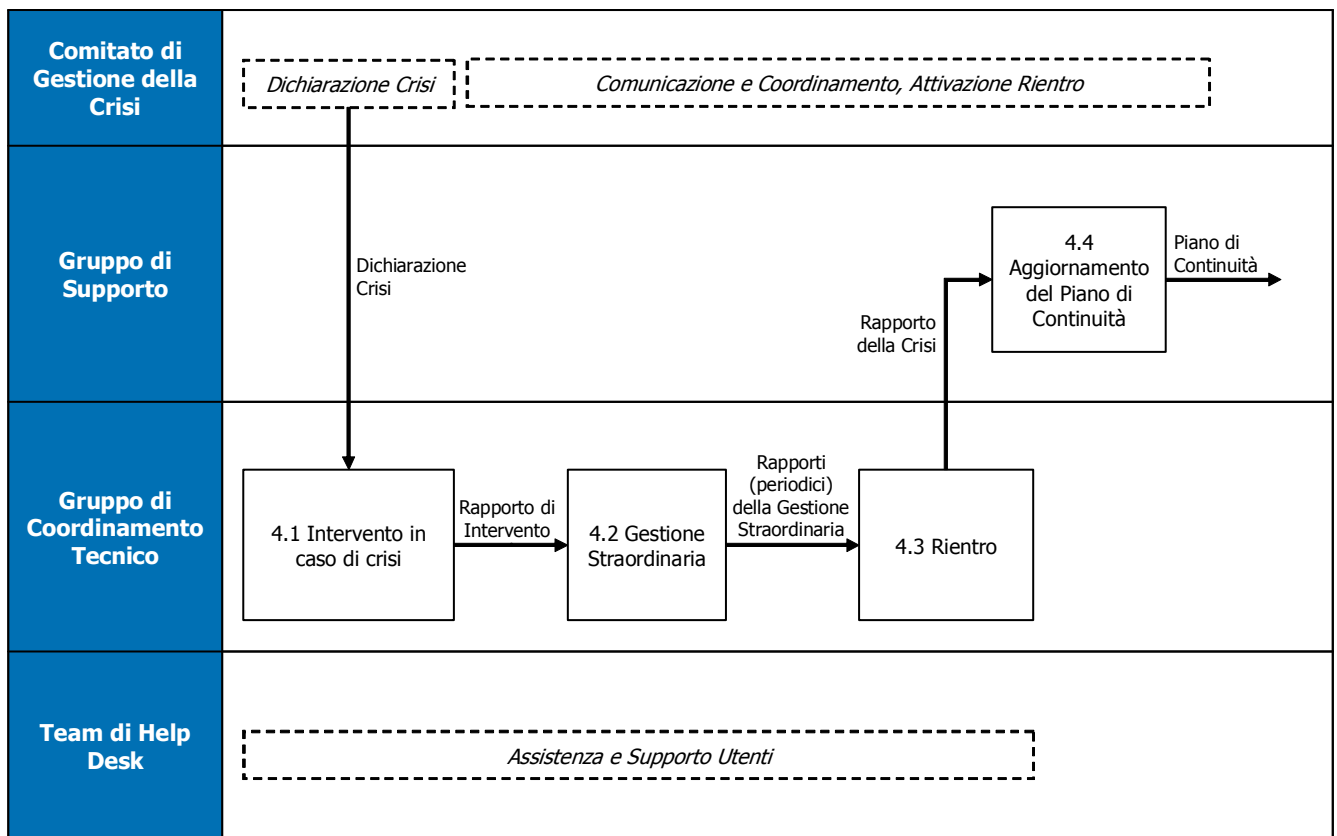


Diagramma 4 – Erogazione del Servizio (Gestione e Manutenzione Straordinaria)

Segue una descrizione di dettaglio delle singole attività.

Intervento in caso di crisi (4.1)

L'attività ha come obiettivo l'esecuzione delle attività necessarie al ripristino di condizioni di continuità operativa a seguito di un evento disastroso, in conformità con gli obiettivi e le modalità di ripristino attesi.

In particolare l'amministrazione potrebbe aver previsto che gli obiettivi RTO ed RPO siano raggiunti anche ad un livello di servizio "degradato" rispetto ai livelli di servizio ottimali in condizioni di gestione ordinaria.

Sono previste le seguenti fasi:

A responsabilità e cura di esecuzione dell'Amministrazione:

- Esecuzione procedure di notifica e attivazione
- Valutazione del danno

A responsabilità e cura di esecuzione del Fornitore:

- Esecuzione sequenza delle azioni di ripristino
- Esecuzione procedure specifiche (di sistema) di ripristino

La modalità di esecuzione di queste fasi e le relative responsabilità tra fornitore ed amministrazione sono concordate e definite nel Piano di Continuità Operativa.

Gestione straordinaria (4.2)

L'attività ha come obiettivo l'esecuzione delle attività di gestione operativa del sistema informatico in regime straordinario, ovvero di soluzione di continuità operativa in essere.

Per queste attività potranno essere utilizzate risorse del Fornitore, risorse dell'amministrazione, ovvero risorse di entrambi in funzione delle esigenze dell'amministrazione stessa e di quanto definito in sede contrattuale.

Il livello di servizio erogato dal fornitore potrà essere – se così determinato e definito dall'amministrazione – in forma “degradata” rispetto al livello di servizio in condizioni di gestione ordinaria.

Rientro (4.3)

L'attività ha come obiettivo il rientro dell'operatività in condizioni normali e la chiusura della gestione straordinaria, ivi compreso il rilascio del sito alternativo eventualmente utilizzato in emergenza.

La modalità di esecuzione di queste attività e le relative responsabilità tra fornitore ed amministrazione sono concordate e definite nel Piano di Continuità Operativa. Tipicamente, le attività includono (in modo non esaustivo):

- assistenza alla amministrazione per il rientro (es. consulenza sulle propedeuticità per il rientro, supporto nella attuazione delle procedure);
- il riportare i dati e le configurazioni dei sistemi dal sito di recovery al sito primario;
- il ripristino delle procedure di allineamento delle configurazioni e dei dati allo stato originale (come appunto previsto nel Piano di Continuità Operatività).

In genere, soprattutto in situazioni contrattuali di collaborazione tra più amministrazioni che prevedano la condivisione del sito alternativo, il Fornitore concorderà con l'amministrazione un periodo massimo di durata della gestione straordinaria ovvero di occupazione del sito alternativo.

Aggiornamento del Piano di Continuità (4.4)

Una sezione specifica del Piano di Continuità dovrà essere dedicato alla conservazione dei “rapporti di crisi”, ove sono dettagliati gli eventi accaduti e gli effetti derivanti, le azioni intraprese ed i risultati ottenuti.

6 DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI

Nella tabella seguente (Matrice di Responsabilità Attività – Profilo Professionale) sono riportati per ciascuna attività i profili professionali EUCIP tipicamente coinvolti nello svolgimento dell'attività stessa e nel rilascio dei relativi prodotti, qualificati in termini di:

- responsabile (**R**), è il profilo professionale che esegue l'attività, coordina gli eventuali contributi di altri profili professionali ed è responsabile primario della qualità dei prodotti dell'attività;
- contributore (**C**), è il profilo professionale che contribuisce con competenze specialistiche allo svolgimento di elementi dell'attività e può gestire in autonomia, in accordo con il responsabile, specifiche sotto-attività; i contributori sono suddivisi in due categorie:
 - contributore tipico (**Ct**), il suo contributo all'attività è richiesto nella quasi totalità delle istanze di fornitura, una sua eventuale assenza dovrebbe essere considerata un'eccezione e le relative motivazioni dovrebbero essere esplicitate (peculiarità tecniche od organizzative dell'istanza di fornitura).
 - contributore specifico (**Cs**), il suo contributo all'attività è legato alle specificità dell'istanza di fornitura, la sua presenza, anche se frequente, non può essere considerata tipica.

Per profilo professionale responsabile (o contributore) si deve intendere non una singola persona fisica, ma una famiglia professionale, caratterizzata da competenze comuni, ove coesistono livelli di esperienza, aree di specializzazione e ruoli organizzativi differenziati.

Ad esempio, è possibile che i Consulenti per la Sicurezza coinvolti nelle strutture organizzative per la gestione della Continuità Operativa (Comitato di Gestione della Crisi, Gruppo di supporto, Gruppo di Coordinamento Tecnico, Team di Help Desk; paragrafo 5.1) siano più d'uno ed in particolare che gli specialisti partecipanti ai team tecnici siano diversi da quello membro del Comitato di Gestione della Crisi.

Nella fase di Analisi e Pianificazione per la Continuità Operativa il profilo professionale responsabile delle attività iniziali di analisi e valutazione è il Revisore di Sistemi Informativi. Le competenze del Revisore di Sistemi Informativi sono particolarmente approfondite in tema di analisi e gestione dei rischi e di sicurezza, sia per gli aspetti tecnici che di impatto sull'operatività dell'organizzazione; il profilo possiede inoltre caratteristiche di indipendenza, autorevolezza e capacità consulenziali indispensabili per coordinare efficacemente le attività di Risk Assessment, Business Impact Analysis e Recoverability Assessment.

Il profilo professionale responsabile della successiva attività di Disegno della Soluzione e del servizio di Continuità Operativa è il Consulente per la Sicurezza che ha competenze estese a tutti gli aspetti di pianificazione della continuità delle attività aziendali ed alla progettazione della relativa soluzione in termini organizzativi, procedurali e tecnici.

Partecipano come contributori alle attività della fase di Analisi e Pianificazione i seguenti profili:

- Analista di Business, collabora al Risk Assessment ed alla Business Impact Analysis valutando in particolare gli elementi di rischio connessi all'operatività dell'Amministrazione ed ai suoi sistemi informativi;
- Progettista di Sistemi Informatici, collabora alle attività di analisi e poi di disegno della soluzione valutando in particolare tutti gli elementi infrastrutturali;
- Responsabile di Basi di Dati, Responsabile di Rete e Responsabile della Configurazione e del Centro Dati, contribuiscono, per le aree di specifica competenza, all'analisi tecnica dei gap esistenti tra situazione corrente ed obiettivi di continuità e partecipano alla progettazione della soluzione atta a colmare tali carenze.

Nella fase di Implementazione (istanza Erogazione del Servizio) i profili professionali responsabili delle attività sono:

- il Responsabile della Configurazione e del Centro Dati, che ha competenze di implementazione e gestione dell'infrastruttura di un centro dati, per la realizzazione e configurazione ed attivazione dell'infrastruttura (partecipa inoltre come contributore alle attività di redazione del piano di continuità e di collaudo dell'infrastruttura);
- il Consulente per la Sicurezza, per la redazione del piano di continuità e le iniziative di comunicazione e formazione agli utenti ed al personale tecnico (partecipa inoltre come contributore all'attività di realizzazione dell'infrastruttura);
- il Tecnico di Collaudo ed Integrazione di Sistemi, per l'attività di supporto all'Amministrazione per il collaudo dell'infrastruttura (partecipa inoltre come contributore all'attività di realizzazione dell'infrastruttura per l'elaborazione del piano di collaudo).

Gli altri profili professionali che contribuiscono alle attività della fase di implementazione tecnica dell'infrastruttura (realizzazione dell'infrastruttura e configurazione ed attivazione) sono il Responsabile di Basi di Dati, il Responsabile di Rete ed il Sistemista Multipiattaforma; il Formatore IT collabora con il Consulente per la Sicurezza per l'attività di comunicazione e formazione degli utenti e del personale tecnico coinvolto nella gestione delle componenti tecnologiche della soluzione di continuità.

Nelle restanti due fasi di erogazione del servizio di continuità operativa, Gestione e Manutenzione del Servizio e Gestione e Manutenzione Straordinaria, i profili professionali coinvolti come responsabili di attività sono:

- il Tecnico di Collaudo e Integrazione di Sistemi, per le attività di esecuzione dei test (primo e periodici) di continuità operativa tesi a verificare l'efficienza nel tempo della soluzione adottata;
- il Consulente per la Sicurezza, per gli aggiornamenti del Piano di Continuità Operativa resisi necessari in seguito a cambiamenti intervenuti nella gestione ordinaria o straordinaria del servizio;
- il Responsabile della Configurazione e del Centro Dati, per le attività di adeguamento della infrastruttura e di gestione straordinaria delle crisi, dalla notifica dello stato di crisi sino al termine del rientro con la ripresa della normale operatività;
- il Supervisore di un Centro di Assistenza, per l'aggiornamento del sistema di conoscenza dell'help-desk.

Collaborano alla gestione ordinaria e straordinaria del servizio, in funzione delle specifiche competenze che caratterizzano il profilo, tutti gli altri specialisti già coinvolti nella fase di implementazione del servizio.

Nella tabella "Matrice di Responsabilità Attività – Profilo Professionale" è anche indicata per ciascun profilo professionale, responsabile (R) o contributore tipico (Ct), un'ipotesi di massima del suo impegno (quantità di lavoro, "effort") nell'attività. Tale impegno è espresso come percentuale, fatto 100 l'impegno totale richiesto dall'attività, ed è quindi una stima del "peso" relativo del profilo professionale nell'esecuzione dell'attività.

L'ampia diversificazione delle possibili soluzioni di continuità adottabili implica margini di variazione significativi dell'impegno dei profili professionali coinvolti in questa classe di fornitura. Le stime sono formulate ipotizzando un'astratta istanza di fornitura tipica, non tengono conto della presenza di eventuali contributori specifici e sono da considerarsi come indicazioni orientative.

TABELLA MATRICE DI RESPONSABILITA' ATTIVITA' – PROFILO PROFESSIONALE (1/2)

	Attività								
	1. Analisi e Pianificazione per la Continuità Operativa				2. Erogazione del Servizio: Implementazione				
Profilo professionale	1.1 Risk Assessment	1.2 Business Impact Analysis	1.3 Recoverability Assessment	1.4 Disegno della Soluzione e del servizio di Continuità Operativa	2.1 Realizzazione dell'Infrastruttura	2.2 Redazione del Piano di Continuità	2.3 Configurazione ed Attivazione	2.4 Comunicazione/ Formazione	2.5 Collaudo dell'Infrastruttura
2 – Revisore di Sistemi Informativi	R 60%	R 60%	R 70%	Ct 10%					
7 – Analista di Business	Ct 20%	Ct 20%							
11- Tecnico di Collaudo e Integrazione di Sistemi					Ct 20%				R 80%
13- Progettista di Sistemi Informatici	Ct 20%	Ct 20%	Ct 10%	Ct 10%					
15 – Consulente per la Sicurezza				R 55%	Ct 5%	R 80%		R 60%	
16 -Responsabile di Basi di Dati			Ct 5%	Ct 5%	Ct 5%		Ct 15%		
17 – Responsabile di Rete			Ct 5%	Ct 5%	Ct 5%		Ct 10%		
18 – Responsabile della Configurazione e del Centro Dati			Ct 10%	Ct 10%	R 50%	Ct 20%	R 60%		Ct 20%
19 – Sistemista Multiplatforma					Ct 15%		Ct 15%		
21 – Formatore IT				Ct 5%				Ct 40%	
% di effort - totale	100%	100%	100%	100%	100%	100%	100%	100%	100%

TABELLA MATRICE DI RESPONSABILITA' ATTIVITA' – PROFILO PROFESSIONALE (2/2)

	Attività								
	3. Erogazione del Servizio: Gestione e Manutenzione del Servizio					4. Erogazione del Servizio: Gestione e Manutenzione Straordinaria			
Profilo professionale	3.1 Esecuzione (primo) Test di Continuità Operativa	3.2 Adeguamento infrastruttura della continuità Operativa	3.3 Aggiornamento del Piano di Continuità	3.4 Esecuzione Test Periodici di Continuità Operativa	3.5 Aggiornamento del Sistema di Conoscenza HelpDesk	4.1 Intervento in caso di crisi	4.2 Gestione straordinaria	4.3 Rientro	4.4 Aggiornamento del Piano di Continuità
11- Tecnico di Collaudo e Integrazione di Sistemi	R 70%	Ct 15%		R 70%					
13- Progettista di Sistemi Informatici									
15 – Consulente per la Sicurezza	Ct 10%	Ct 10%	R 80%	Ct 10%	Ct 10%				R 80%
16 -Responsabile di Basi di Dati		Ct 10%				Ct 20%	Ct 20%	Ct 20%	
17 – Responsabile di Rete		Ct 5%				Ct 10%	Ct 10%	Ct 10%	
18 – Responsabile della Configurazione e del Centro Dati	Ct 20%	R 50%	Ct 20%	Ct 20%	Ct 10%	R 60%	R 40%	R 60%	Ct 20%
19 – Sistemista Multiplatforma		Ct 10%				Ct 10%	Ct 10%	Ct 10%	
20 – Supervisore di un Centro di Assistenza					R 80%		Ct 20%		
21 – Formatore IT		Cs							
% di effort - totale	100%	100%	100%	100%	100%	100%	100%	100%	100%

I profili professionali di riferimento sono quelli definiti dallo schema EUCIP (European Certification of Informatics Professionals) sviluppato dal CEPIS (Council of European Professional Informatics Societies) che, per ciascun profilo, indica le attività tipiche ed il dettaglio delle competenze possedute.

Le sintesi delle competenze dei profili professionali coinvolti nelle attività di questa classe di fornitura sono le seguenti (tra parentesi l' identificativo del profilo):

(2) Revisore di Sistemi Informativi (Information Systems Auditor). Un revisore di sistemi informativi secondo lo standard EUCIP fornisce (riferendo ai più alti responsabili aziendali o agli organi direttivi) un livello indipendente di garanzia su sicurezza, qualità, conformità e valore aggiunto dei sistemi informativi in una particolare organizzazione. Deve dimostrare forti competenze tecniche, indipendenza di giudizio, aderenza all'etica professionale.

(7) Analista di Business (Business Analyst). Un analista di business secondo lo standard EUCIP deve essere molto efficace nel cogliere il caso aziendale, definirne i requisiti, modellarne i processi gestionali e nell'identificare una tipologia adeguata di soluzioni ICT. Un atteggiamento professionale di alto livello e l'abilità nel comunicare sono in per questo ruolo altrettanto essenziali quanto una competenza dell'ICT ampia e approfondita.

(11) Tecnico di Collaudo e Integrazione di Sistemi (Systems Integration & Testing Engineer). Un tecnico di collaudo e integrazione di sistemi secondo lo standard EUCIP deve essere molto efficace in varie aree dello sviluppo di sistemi: preparazione della documentazione per l'utente finale, allestimento di sistemi IT, test delle loro funzioni, sia nel complesso che per singoli moduli componenti, identificazione delle anomalie e diagnosi delle possibili cause. E' richiesta anche una conoscenza specifica su come vengono costruite le interfacce tra moduli software.

(13) Progettista di Sistemi Informatici (IT Systems Architect). Un progettista di sistemi informatici secondo lo standard EUCIP assume un ruolo centrale nella progettazione, integrazione e miglioramento di sistemi IT – con particolare riguardo alle architetture software – curandone anche la sicurezza e le prestazioni; oltre ad una vasta competenza dell'ICT (in tutti i campi: software, hardware e reti) e di tecniche di progettazione specifiche, è richiesta la capacità di descrivere un sistema in termini di componenti e flussi logici.

(15) Consulente per la Sicurezza (Security Adviser). Un consulente per la sicurezza secondo lo standard EUCIP deve essere molto efficace nell'identificare i requisiti di sicurezza dei sistemi ICT e nel definire soluzioni affidabili e agevoli da gestire. Ad una competenza dell'ICT ampia e approfondita deve essere abbinata la capacità di interagire con altre funzioni ICT per favorire l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura ICT.

(16) Responsabile di Basi di Dati (Database Manager). Un responsabile di basi di dati secondo lo standard EUCIP assume un ruolo centrale tanto nella progettazione di strutture di dati quanto nella gestione ordinaria dei DB; tra i requisiti figurano dunque una profonda competenza in tutti gli aspetti delle tecnologie dei DB, un approccio collaborativo ai contesti di progetto, esperienza nelle tecniche di modellazione dei dati, ma anche l'efficacia nel definire e applicare le procedure e nell'organizzare le operazioni ordinarie.

(17) Responsabile di Rete (Network Manager). Un responsabile di rete secondo lo standard EUCIP deve essere molto efficace nel gestire un sistema informativo di rete di media complessità e nel migliorarne le prestazioni. Deve inoltre saper interagire con i progettisti di reti e con eventuali fornitori esterni in merito a tutte le fasi del ciclo di vita di una rete.

(18) Responsabile della Configurazione e del Centro Dati (Data Centre & Configuration Manager). Un responsabile della configurazione e del centro dati secondo lo standard EUCIP deve avere un approccio strutturato alla progettazione, allestimento e manutenzione di un ambiente di lavoro supportato dall'IT, sia nel caso di un ambiente di sviluppo, sia nel caso di un sistema "in produzione" destinato agli utenti finali; è richiesta una particolare competenza sulle procedure di qualità e su strumenti e sistemi di gestione procedurale delle attività.

(19) Sistemista Multiplatforma (X-Systems Engineer). Un sistemista multiplatforma secondo lo standard EUCIP deve avere una particolare competenza su vari sistemi operativi e sui rispettivi metodi per affrontare i problemi, sull'ottimizzazione delle prestazioni, sulla programmazione a livello di sistema e sull'integrazione tra piattaforme diverse; l'attitudine alla diagnosi e alla risoluzione dei problemi è richiesta per dare supporto su sistemi proprietari o aperti e su configurazioni ibride.

(20) Supervisore di un Centro di Assistenza (Help Desk Supervisor). Un supervisore di un centro di assistenza secondo lo standard EUCIP deve essere efficace nel fornire supporto tecnico; ciò richiede competenza di una tecnologia specifica (legata al contesto, es. servizi in rete), ma anche dimestichezza con contratti SLA, consapevolezza delle priorità operative nell'attività del cliente e delle problematiche tipiche degli utenti, così come un atteggiamento positivo nel reagire ai problemi e nel rapportarsi con il cliente.

(21) Formatore IT (IT Trainer). Un formatore IT secondo lo standard EUCIP deve essere molto efficace nel comunicare concetti IT, nell'addestrare gli utenti e nel motivarli a utilizzare al meglio i sistemi IT; tra i requisiti figurano un'ampia cultura ICT, una specializzazione su una particolare tecnologia (legata al contesto, es. prodotti IT per la collaborazione), un'eccellente capacità di esposizione e la padronanza delle tecniche didattiche, comprensive della progettazione e preparazione di materiale efficace.

7 INDICATORI/MISURE DI QUALITÀ

La tabella a partire dalla pagina seguente (Tab.1), associa ad ogni attività e/o prodotto della fornitura gli indicatori di pertinenza descritti nelle schede successive.

Tabella 1 - Attività / Prodotti / Indicatori
Analisi e Pianificazione (1)

Attività	Prodotto	Indicatore di Qualità (IQ)				Processo Trasversale (PT)		
		Caratteristica	Sottocaratteristica	Acro IQ	Denominazione IQ	Cod PT	Acro PT	Denominazione PT
1.1 Risk assessment	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Relazione di valutazione del rischio	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
1.2 Business Impact Analysis	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Relazione di analisi di impatto	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
1.3 Recoverability Assessment	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Relazione Recoverability Assessment	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
1.4 Disegno della Soluzione e del servizio di Continuità Operativa	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Relazione Tecnica del servizio di Continuità Operativa	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione

Tabella 1 - Attività / Prodotti / Indicatori
Erogazione del Servizio / Implementazione (2)

Attività	Prodotto	Indicatore di Qualità (IQ)				Processo Trasversale (PT)		
		Caratteristica	Sottocaratteristica	Acro IQ	Denominazione IQ	Cod PT	Acro PT	Denominazione PT
2.1 Realizzazione dell'infrastruttura	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
2.2 Redazione del Piano di Continuità	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Piano di Continuità Operativa (ICT)	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
	Piano di Continuità Operativa (ICT)	Usabilità	Comprensibilità	CLC	Completezza e Livello di Comprensibilità			
2.3 Configurazione ed attivazione	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
2.4 Comunicazione / Formazione	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	(attività)	Efficacia	Efficacia	EDD	Efficacia Didattica del Docente	1.3.2	FOR	Formazione e Addestramento
2.5 Collaudo dell'infrastruttura	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Piano di Collaudo	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione

Tabella 1 - Attività / Prodotti / Indicatori
Erogazione del Servizio / Gestione e Manutenzione del Servizio (3)

Attività	Prodotto	Indicatore di Qualità (IQ)				Processo Trasversale (PT)		
		Caratteristica	Sottocaratteristica	Acro IQ	Denominazione IQ	Cod PT	Acro PT	Denominazione PT
3.1 Esecuzione (primo) Test di Continuità Operativa	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Relazione Esito Test	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
	(attività)	Efficacia	Efficacia	RXO	Raggiungimento dell'obiettivo "Tempo di ripristino sul Sito di Recovery"			
3.4 Esecuzione Test Periodici di Continuità Operativa	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Relazione Esito Test	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
	(attività)	Efficacia	Efficacia	RXO	Raggiungimento dell'obiettivo "Tempo di ripristino sul Sito di Recovery"			
3.2 Adeguamento infrastruttura della Continuità Operativa	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
3.3 Aggiornamento del Piano di Continuità	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Piano di Continuità Operativa ICT	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
	Piano di Continuità Operativa (ICT)	Usabilità	Comprensibilità	CLC	Completezza e Livello di Comprensibilità			
3.5 Aggiornamento del Sistema di Conoscenza Help Desk	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione

Numero d'Oggetto/Part Number
MANUALE 4

Ed./Issue Data/Date
2.1 26.03.2009

Com. Mod./Ch. Notice

3.3.3 COP Continuità Operativa

Tabella 1 - Attività / Prodotti / Indicatori
Erogazione del Servizio / Gestione e Manutenzione Straordinaria (4)

Attività	Prodotto	Indicatore di Qualità (IQ)				Processo Trasversale (PT)		
		Caratteristica	Sottocaratteristica	Acro IQ	Denominazione IQ	Cod PT	Acro PT	Denominazione PT
4.1 Intervento in caso di crisi (*)	(attività)	Efficacia	Efficacia	RXO	Raggiungimento dell'obiettivo "Tempo di ripristino sul Sito di Recovery"			
4.2 Gestione Straordinaria	(attività)	Affidabilità	Tolleranza	SGS	Mantenimento SLA della Gestione Straordinaria			
	Registro di Conduzione Operativa (Rapporto della Gestione Straordinaria)	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
4.3 Rientro	(attività)	Funzionalità	Adeguatezza	CRAC	Correttezza dell'aggiornamento della configurazione	6.1.2	PGC	Gestione della configurazione
4.4 Aggiornamento del Piano di Continuità	(attività)	Efficienza	Efficienza Temporale	RSC	Rispetto della Scadenza Contrattuale	6.2.1	PGE	Gestione
	Piano di Continuità Operativa ICT	Funzionalità	Accuratezza	RSD	Rispetto degli Standard Documentali	6.1.1	PGD	Documentazione
	Piano di Continuità Operativa (ICT)	Usabilità	Comprensibilità	CLC	Completezza e Livello di Comprensibilità			

(*) Oltre agli indicatori RTO ed RPO, valgono tutti gli indicatori di SLA correnti sul perimetro oggetto della continuità operativa sui sistemi primari (definiti in fase di analisi); ciò, a meno di non aver previsto SLA specifici della gestione straordinaria (tipicamente "degradati") nel Piano della Continuità Operativa.

Tabella 2 – Dettaglio Indicatori e Misure
Completezza e Livello di Comprensibilità / CLC

Classe di fornitura	CONTINUITA' OPERATIVA
Caratteristica / Sottocaratteristica	Usabilità / Comprensibilità.
Indicatore / Misura	Completezza e Livello di Comprensibilità / CLC.
Sistema di gestione delle misure	L'indicatore misura il livello di completezza (incluso il livello di aggiornamento) e di comprensibilità del Piano di Continuità ICT. Poiché le attività e gli aspetti organizzativi legati ad un intervento in caso di crisi sono descritti in tale documento, la sua comprensibilità ed immediatezza d'uso sono alla base del successo delle azioni di ripristino in caso di disastro.
Unità di misura	Percentuale.
Dati elementari da rilevare	Attraverso un'attività di "Verifica teorica", sono rilevati: <ul style="list-style-type: none"> • Numero di paragrafi di secondo livello (es. x.y) complessivi • Numero di paragrafi di secondo livello giudicati non comprensibili (dove per non comprensibilità si intende l'assenza di chiarezza rispetto ad uno qualsiasi dei seguenti argomenti: identificazione dei componenti oggetto dell'attività, attività, ruoli, responsabilità, risultati, propedeuticità, tempistica). <p>In caso di esecuzione della misura a valle di un Test di Continuità Operativa, il "Numero di paragrafi di secondo livello giudicati non comprensibili" è dato dai paragrafi il cui esito effettivo è stato difforme da quanto atteso nel documento.</p>
Periodo di riferimento	Non applicabile.
Frequenza esecuzione misure	La misura è effettuata ad ogni aggiornamento del Piano di Continuità ICT (incluso in sede di prima stesura).
Regole di campionamento	La misura si applica, secondo il caso: <ul style="list-style-type: none"> • sulla totalità del contenuto del Piano di Continuità ICT; • sul contenuto del Piano di Continuità ICT oggetto di Test di Continuità Operativa; • sul contenuto del Piano di Continuità ICT oggetto di aggiornamento.
Formula di calcolo	Dati necessari: NPT = numero di paragrafi di secondo livello (es. x.y) complessivi; NPN = numero di paragrafi di secondo livello (es. x.y) giudicati non comprensibili (o non operabili correttamente). $CLC = 100 \times (NPN / NPT)$
Regole di arrotondamento	Secondo decimale (es. nnn,dd%; 7,505 = 7,51 e 7,504 = 7,50).
Obiettivi (valori soglia)	CLC = 0 (il documento deve essere completamente comprensibile).
Azioni contrattuali	Si richiede l'adeguamento tempestivo entro 5 giorni lavorativi dalla rilevazione di superamento del valore soglia.
Eccezioni	Qualora il superamento del valore soglia sia dovuto a cambiamenti (organizzativi, tecnologici e/o di processo) non comunicati al fornitore, l'adeguamento potrà avvenire entro 15 giorni lavorativi dalla comunicazione del cambiamento stesso (a cura del committente).

Tabella 2 – Dettaglio Indicatori e Misure
Raggiungimento dell'obiettivo "Tempo di ripristino sul Sito di Recovery"

Classe di fornitura	CONTINUITA' OPERATIVA
Caratteristica / Sottocaratteristica	Efficacia / Efficacia.
Indicatore / Misura	Tempo di ripristino sul sito di backup
Sistema di gestione delle misure	<p>Oggetto della misura sono:</p> <ol style="list-style-type: none"> (RTOE) il tempo di ripristino sul sito di recovery (ovvero su ambiente di test dedicato presso il sito di recovery, se previsto sulla base delle caratteristiche e funzionalità dei sistemi informatici), misurato come l'intervallo di tempo massimo entro il quale le risorse (oggetto contrattuale della continuità operativa) necessarie alla erogazione del servizio IT risultano disponibili all'uso presso il sito di recovery e conformi ai livelli di servizio concordati negli obiettivi contrattuali (l'intervallo di tempo viene misurato a partire dal momento della dichiarazione di disastro in sede di test simulato); (RPOE) la verifica del livello di allineamento dei dati tra i sistemi del sito primario ed i sistemi del sito di recovery, secondo le specifiche contrattuali e quanto meglio specificato nel piano di continuità operativa; in particolare, i dati sul sito di recovery devono risultare disponibili e consistenti con i dati sul sito primario all'istante di allineamento tra i dati richiesto. <p>Il raggiungimento dell'obiettivo è calcolato come distanza (temporale) tra i valori RTOE (RPOE) misurati ed i valori RTOA (RPOA) attesi e richiesti in sede contrattuale.</p> <p>I valori sono rilevati in un contesto simulato di crisi, selezionato tra gli scenari di disastro previsti nel piano di continuità operativa (è possibile effettuare la misura nel caso di uno o più scenari tra quelli previsti, eventualmente – per ragioni di costo e/o di tempo – applicati su un sottoinsieme del perimetro informatico oggetto contrattuale delle continuità operativa).</p>
Unità di misura	Intervallo di tempo
Dati elementari da rilevare	<p>NT = Data (gg/mm/aaaa) e ora (hh:mm:ss) di notifica dell'evento disastroso. DS = Data (gg/mm/aaaa) e ora (hh:mm:ss) di disponibilità all'uso dei sistemi. UP = Data (gg/mm/aaaa) e ora (hh:mm:ss) ultimo punto di consistenza dei dati e dei file system (dati consistenti e validi). RTOA = RTO atteso (sono possibili RTOA distinti per diversi sottosistemi informatici). RPOA = RPO atteso (sono possibili RPOA distinti per diversi sottosistemi informatici).</p>
Periodo di riferimento	Secondo la pianificazione dei Test prevista contrattualmente e dettagliata nel piano di continuità operativa
Frequenza esecuzione misure	La misura è effettuata nei casi di Test di Continuità Operativa eseguiti nella modalità "Simulazione".
Regole di campionamento	<p>La misura si applica al perimetro dei sistemi informatici oggetto del contratto di servizio di continuità operativa, e viene effettuata periodicamente in sede di primo test di continuità operativa e test periodici successivi.</p> <p>Il perimetro di dettaglio sul quale applicare le regole, le misure e gli obiettivi dei test di continuità operativa sono definiti in sede di predisposizione del piano di test conformemente alle specifiche contrattuali correnti (inclusi eventuali aggiornamenti successivi) e con le operatività specificate nel piano di continuità operativa.</p> <p>In presenza di obiettivi RTOA ed RPOA diversificati per sottosistema informatico, dovranno essere rilevate misure specifiche RTOE ed RPOE per ogni sottosistema oggetto del test di continuità operativa.</p>

8 GLOSSARIO

Analisi del rischio. Attività volta a identificare minacce e vulnerabilità di un sistema, allo scopo di definirne gli obiettivi di sicurezza e di permettere la gestione del rischio.

ANS (Autorità Nazionale per la Sicurezza). Il Presidente del Consiglio dei Ministri ovvero l'Organo dallo stesso delegato per l'esercizio delle funzioni in materia di tutela delle informazioni, documenti e materiali classificati; (DPCM 11 aprile 2002).

Attivazione. L'implementazione delle funzionalità di Continuità Operativa, delle procedure, delle attività e piani in risposta a una emergenza di Continuità Operativa, a un evento, un Incidente e/o una Crisi.

BS7799. Standard del BSI per la realizzazione, valutazione e certificazione di un sistema di gestione della sicurezza delle informazioni. Consiste di due parti: la prima - diventata norma ISO/IEC 17799 - contiene le raccomandazioni per una corretta gestione della sicurezza di sistema o di processo, mentre la seconda parte specifica i requisiti per la realizzazione di un ISMS. La sezione 9 tratta la Gestione della Continuità Operativa.

BSI. Acronimo di British Standard Institution. Ente costituito dal Dipartimento del Commercio e Industria del governo inglese con l'intento di sostenere, indirizzare e mantenere la qualità dell'industria britannica.

Business Continuity Management (BCM). Un processo di gestione olistica che identifica impatti potenziali che minacciano un'organizzazione nel suo insieme e che fornisce una struttura con la capacità di offrire una risposta efficace che salvaguardi gli interessi aziendali, la sua reputazione, il marchio e le sue attività.

Certificazione di sistemi di gestione della sicurezza ICT (Information Security Management Systems – ISMS). Oggetto della certificazione è il processo mediante il quale un'organizzazione gestisce la sicurezza ICT al suo interno. La norma di riferimento è rappresentata dallo standard britannico BS7799, la cui parte introduttiva, non utilizzabile ai fini della certificazione, è stata adottata dall'ISO/IEC (IS 17799). In Italia il Sincert (Sistema Nazionale per l'Accreditamento degli Organismi di Certificazione e Ispezione) ha sviluppato uno Schema per l'accreditamento di Organismi di certificazione ai quali viene affidato il compito di verificare il soddisfacimento dei requisiti contenuti nella norma.

Cold site. Centro di elaborazione d'emergenza che dispone dei componenti e delle infrastrutture elettriche di un sistema di produzione normale, ma non contiene i computer. Il sito è pronto per accogliere i computer quando occorre passare dal centro di calcolo principale a quello di riserva, in caso di disastro.

Comitato di gestione della crisi (o Comitato di crisi). Organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività degli altri gruppi coinvolti nella continuità operativa. Tra i suoi compiti: l'approvazione del piano di continuità operativa, la dichiarazione dello stato di crisi, l'avvio delle attività di rientro alle condizioni normali, i rapporti con l'esterno e le comunicazioni ai dipendenti.

Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni. Comitato istituito con Decreto Interministeriale (Min. Comunicazioni e Min. Innovazione e Tecnologie) del 24 luglio 2002, avente funzioni di indirizzo e coordinamento delle iniziative in materia di sicurezza nelle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni. Nell'aprile 2004, il Comitato ha pubblicato le "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la pubblica amministrazione".

Continuità operativa. Insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery.

Copia dei dati. Un processo con cui dati ritenuti critici vengono copiati in un'altra locazione, in modo che non vengano persi nell'evento di perdita di Continuità Operativa. Può essere utilizzata come soluzione di Disaster Recovery effettuando la copia remotamente. Esistono funzioni di copia dati a livello hardware e a livello software.

Crisi. Un evento o una percezione che minaccia le operazioni, il personale, il valore dell'azienda, il nome, la reputazione e/o gli obiettivi strategici di una organizzazione.

D.P.C.M. 16 gennaio 2002. Decreto contenente indicazioni per le Pubbliche Amministrazioni statali in materia di sicurezza informatica e delle telecomunicazioni. Riporta in allegato uno schema di autovalutazione dello stato della sicurezza informatica e l'organizzazione a cui le PA devono tendere per realizzare una "base minima di sicurezza".

Database Replication. Duplicazione parziale o totale dei dati da un database sorgente a uno o più database destinatari. Il processo di replica può utilizzare svariate metodologie (data mirroring) e può essere eseguito in modalità sincrona, asincrona o a tempi specifici, a seconda delle tecnologie utilizzate, dei requisiti di recupero richiesto, della distanza e della connettività esistente verso il database sorgente. La replica, se eseguita remotamente, può funzionare come backup per situazioni catastrofiche e altri outage di grandi entità.

Disaster Recovery. Insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.

Disastro. Una calamità improvvisa e non pianificata che causa gravi danni o perdite. Tipicamente implica l'inizio del trasferimento dal sito primario ad una località secondaria.

Emergenza. Una situazione reale o imminente (tanto da rappresentare una minaccia), che possa causare lesioni, morti, distruzione di proprietà e/o interruzione delle normali attività operative di una azienda.

Gestione del rischio. Attività volta a individuare le contromisure logiche, fisiche, organizzative e amministrative per soddisfare gli obiettivi di sicurezza e contrastare i rischi individuati dall'analisi del rischio.

Hot site. Un sito di riserva (centro di elaborazione dati, area di lavoro) che fornisce funzioni di Business Continuity Management equipaggiato con hardware e software, interfacce per le telecomunicazioni e uno spazio controllato in grado di fornire supporto di elaborazione dati alternativo in tempi relativamente immediati per mantenere la attività critiche dell'organizzazione. Pronto all'uso in caso di evento catastrofico al centro primario.

Outage. Periodo di tempo in cui un servizio, un sistema, un processo o una funzione operativa è inaccessibile o inusabile, comportando un alto impatto sull'organizzazione, compromettendo il raggiungimento degli obiettivi operativi dell'organizzazione stessa. L'outage è diverso dal "downtime", in cui fermi di processo o di sistema avvengono come parte della normale operatività, e il cui l'impatto riduce semplicemente l'efficienza a breve termine dei processi.

Piano di continuità operativa. Documento di progettazione e pianificazione delle attività di continuità operativa, contenente le misure di carattere operativo da adottare per attuare le gestione della situazione di emergenza crisi e il successivo ripristino della normale operatività.

Ripristino. Attività che consiste nel riportare un sistema al suo stato precedente a un errore. Nel caso di perdita di dati, permette di rigenerarli come erano prima dell'evento, in genere partendo da un backup.

Rischio. Possibilità che un determinato evento avverso causi un danno a un bene, sfruttandone i punti deboli. Di solito si misura combinando l'impatto e la probabilità di accadimento. In senso generale può essere definito come la minaccia di una azione o una non-azione che potrebbe impedire a una organizzazione il raggiungimento degli obiettivi operativi.

Sistema di gestione della sicurezza delle informazioni. Parte del sistema di gestione del sistema informativo di un'organizzazione basato sul rischio per definire, realizzare, esercitare, monitorare, mantenere e migliorare il processo di sicurezza delle informazioni.

Sistema informatico. Insieme delle tecnologie informatiche a supporto dell'automazione del sistema informativo.

Sistema informativo. Insieme delle attività di elaborazione manuale e automatizzata dei dati, dei processi informativi, delle relative risorse umane e tecnologiche e dell'infrastruttura fisica di riferimento.

Sito duplicato (ridondato). Sito alternativo, anche condiviso con un'altra realtà. A differenza dell'hot site, è un sito sempre attivo. Anche conosciuto come Sito di Recovery.

Sito di recovery. Sito mantenuto in stato di allerta e utilizzato in situazioni di mantenimento della Continuità Operativa.

Test. Una attività in cui vengano seguite alcune parti di un piano di Continuità Operativa per assicurarsi che il piano contenga le informazioni appropriate per produrre i risultati attesi. Un test si differenzia da un'esercitazione in quanto un test si effettua presso un sito alternativo, mentre una esercitazione è generalmente una simulazione.