

Scheda descrittiva della pratica tecnologica ed organizzativa

Strumenti e metodologie per la Continuità Operativa ed il Disaster Recovery cedute in riuso

Consiglio Regionale del Piemonte

1 GENERALITÀ

1.1 Identificazione e classificazione dell'amministrazione cedente

➔ Amministrazione cedente: **Consiglio Regionale del Piemonte**

➔ Amministrazione cedente - Sigla : **CRP**

➔ Tipologia di Amministrazione cedente: **Amministrazione regionale**

1.2 Descrizione sintetica della pratica ceduta in riuso

Strumenti e metodologie per la realizzazione del Piano di Continuità Operativa e Disaster Recovery

1.3 Tipologia di Pratica offerta in riuso

Metodologia

1.4 Referenti dell'amministrazione cedente

➔ Referente/i della Pratica	• Nome e cognome:	Elena Fenoglio
	• Indirizzo:	Via Arsenale ,12 10121 Torino
	• Tel/Cel:	011 5757480
	• e-mail::	<i>elena.fenoglio@cr.piemonte.it</i>

➔ Referente amministrativo	• Nome e cognome:	Elena Fenoglio
	• Indirizzo:	Via Arsenale ,12 10121 Torino
	• Tel/Cel:	011 5757480
	• e-mail::	<i>elena.fenoglio@cr.piemonte.it</i>

2 SCENARIO DI RIUSO

2.1 Descrizione dettagliata della pratica ceduta in riuso

Gli strumenti ed i metodi di analisi utilizzati per la definizione del Piano di Continuità Operativa e del Disaster Recovery, intesi come *know how* tecnologico ed organizzativo, sono resi disponibili ad ogni Ente che debba ottemperare alla normativa in merito alla continuità del servizio (nuovo Codice Amministrazione Digitale), e anche per la realizzazione dell'outsourcing dei propri sistemi informativi.

Gli strumenti e i metodi predisposti consentono di intervenire su:

- **Predisposizione della documentazione per l'acquisizione del parere dell'Agenzia per l'Italia Digitale.**

Strumento organizzativo di supporto per la predisposizione della documentazione per l'acquisizione del parere dell'Agenzia per l'Italia Digitale (Supporto per analisi infrastrutture ICT dell'Ente – Supporto per la redazione delle schede di Autovalutazione – Business Impact Analysis - Supporto per la redazione dello Studio di Fattibilità Tecnica).

- **Progettazione organizzativa/procedurale e tecnologica di dettaglio per il Piano di Continuità Operativa e Disaster Recovery**

La fase di progettazione si compone di due sotto-servizi, e fornisce il supporto all'Ente:

- nella definizione del progetto di dettaglio del modello organizzativo/procedurale per la realizzazione del Piano di Continuità Operativa
- nella individuazione delle soluzioni tecnologiche necessarie per l'approvvigionamento e la messa in opera delle soluzioni di replica dati e di Disaster Recovery

In questa fase si approfondiscono le tematiche introdotte nel progetto organizzativo/procedurale di alto livello, con la definizione di dettaglio dei ruoli, delle singole responsabilità, delle modalità di intervento e di quanto altro necessario a rendere operativo il modello organizzativo/procedurale.

- **Piano di Continuità Operativa**

Il Piano di Continuità Operativa fissa gli obiettivi, descrive i ruoli, le responsabilità, i sistemi di escalation e le procedure per la gestione dell'emergenza, tenuto conto delle potenziali criticità relative a risorse umane, strutturali e tecnologiche.

Elemento essenziale nella fase di realizzazione del Piano, sono i dati emersi dalla Business Impact Analysis (BIA/RA). Tali dati permetteranno quindi di identificare, quantificare e qualificare gli impatti in caso di perdita, interruzione o arresto dei processi e dei servizi dell'Ente, fornendo le basi sulle quali definire un'appropriata strategia di Continuità Operativa e Disaster Recovery.

- **Aggiornamento del Piano di Continuità Operativa**

La revisione periodica del Piano di Continuità Operativa deve essere programmata con una frequenza tale da individuare le eventuali variazioni organizzative.

L'aggiornamento del Piano di Continuità Operativa costituisce l'insieme delle attività che periodicamente devono essere effettuate per assicurare la validità del Piano stesso nel corso del tempo.

L'Ente può decidere in completa autonomia quando effettuare le attività previste dal servizio in oggetto, e procedere quindi con l'attivazione del servizio a fronte di importanti modifiche organizzative ovvero per ottemperare alle verifiche periodiche imposte dal Codice di Amministrazione Digitale in materia di Continuità Operativa.

- **Redazione delle procedure di Disaster Recovery**

La redazione delle procedure di Disaster Recovery (o Piano di Disaster Recovery) che costituisce parte integrante del Piano di Continuità Operativa, stabilisce le misure tecniche ed organizzative per garantire il funzionamento dei centri elaborazione dati e delle procedure informatiche in siti alternativi a quelli di produzione. Seguendo le specifiche metodologie di riferimento è prevista l'esecuzione in maniera strutturata delle seguenti fasi:

- Definizione e redazione delle procedure ICT per l'attivazione delle infrastrutture e dei servizi ICT nel Data Center secondario e per il successivo ritorno alla normalità
- Piano dei Test
- Supporto per la realizzazione dei Test

- **Mantenimento e gestione delle soluzioni ICT a supporto del Piano di Disaster Recovery in condizioni di normale operatività**

Come da normativa e metodologie di riferimento, le attività annuali per il mantenimento del Piano di Disaster Recovery sono necessarie per evitare il progressivo "degrado" delle procedure in esso contenute, che porterebbe in un lasso di tempo molto breve alla completa inutilità del Piano stesso.

Si tratta quindi di un supporto all'Ente nella gestione delle procedure DR in condizioni di normale operatività.

La gestione e il mantenimento del Piano di Disaster Recovery costituisce l'insieme delle attività che periodicamente devono essere effettuate per assicurare la validità del Piano stesso nel corso del tempo, con l'obiettivo di:

- verificare la rispondenza del Piano alle esigenze dell'Ente
- pianificare i test del Piano
- verificare la validità dei test stessi a prove ultimate

- **Gestione delle soluzioni ICT a supporto del PIANO DR in condizioni di emergenza**

Di esclusiva competenza degli ambienti informatici in esercizio a supporto del Piano DR, prevede l'esecuzione di tutte le attività, informatiche e non, previste nel Piano di Disaster Recovery per attivare l'erogazione dei servizi nel CED secondario a fronte del verificarsi di un evento che abbia reso non operativo il CED primario dell'Ente, e tutte le attività, informatiche e non, necessarie per il rientro alla normalità al termine del periodo di crisi (spegnimento delle infrastrutture ICT del CED secondario e riattivazione delle infrastrutture del CED primario).

Queste attività quindi coinvolgeranno tutte le infrastrutture ICT a supporto del Piano dell'Ente, la componente di rete e la soluzione di replica dei dati.

- **Business Continuity assessment**

Si tratta di un metodo di analisi in grado di individuare la distanza tra una situazione reale e gli specifici requisiti previsti da una norma o da una metodologia. Il risultato di

questa analisi è la descrizione delle attività e degli elementi necessari per azzerare o per ridurre in modo significativo questa distanza.

L'attività di analisi sui processi organizzativi dell'Ente ha l'obiettivo di evidenziare le criticità che si potrebbero incontrare nella realizzazione di un Piano di Continuità Operativa e di Disaster Recovery.

L'analisi è finalizzata a:

- Individuare gli elementi di criticità per la continuità dei servizi dell'Ente
- Indicare le opportune azioni correttive
- Predisporre un piano di azione per l'eventuale realizzazione dei Piani di Continuità Operativa e di Disaster Recovery.

- **Data Center Facility assessment**

L'attività di analisi sul Data Center e sull'architettura ICT dell'Ente, si pone l'obiettivo di evidenziare eventuali criticità che giustifichino l'esecuzione di interventi di consolidamento/adeguamento per aumentare l'affidabilità complessiva del Data Center dell'Ente.

I risultati di questa analisi possono portare ad una riduzione dei costi e ad un aumento dell'affidabilità intrinseca della Server Farm dell'Ente sia per l'erogazione dei servizi in periodo normale, sia in ottica di Disaster Recovery.

Soprattutto per quest'ultima ipotesi il consolidamento delle infrastrutture ICT diminuisce drasticamente la complessità delle procedure di replica e ripristino delle infrastrutture sul CED secondario, aumentando di conseguenza la probabilità di successo nel caso sia necessario attivare le procedure di Disaster Recovery.

2.2 Destinatari della pratica ceduta in riuso

Le pratiche tecnologiche ed organizzative descritte sono state utilizzate a diversi livelli da Enti appartenenti alla pubblica amministrazione piemontese, tra i quali:

- Consiglio Regionale del Piemonte
- Regione Piemonte
- Università di Torino
- Università del Piemonte Orientale
- Provincia di Torino
- Provincia di Vercelli
- Comune di Torino
- Comune di Pinerolo
- Comune di Nichelino
- Comune di Rivalta
- Comune di Galliate
- ARPEA (Agenzia Regionale Piemontese per le Erogazioni in Agricoltura)
- Azienda Ospedaliera Città della Salute

Alla pratica qui descritta hanno mostrato interesse le seguenti amministrazioni:

- Regione Abruzzo
- Comune di Milano
- Comune di Bari

2.3 Ambito amministrativo interessato

- Gestione sistemi informativi (ICT)
- **Altro:** Tutti i processi amministrativi dell'Ente

2.4 Contesto organizzativo

Per la Pubblica Amministrazione la Continuità Operativa è un dovere perché:

- E' tenuta ad assicurare la continuità dei propri servizi per garantire il corretto svolgimento delle funzioni pubbliche ed il diritto dei cittadini ad accedere ai servizi pubblici per via telematica (art. 3, D.lgs. 82/2005, "Codice dell'Amministrazione Digitale")
- L'Art. 97 della Costituzione ed il principio di buon andamento dell'amministrazione devono essere garantiti anche se si utilizzano tecnologie ICT a supporto dei procedimenti
- La normativa in merito alla Continuità Operativa per gli Enti della PA all'interno del nuovo CAD (art. 50-bis del Dlgs 30 dicembre 2010 , n. 235 - Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82), ed in particolare le "Linee guida per il Disaster Recovery della PA" emesse dall'Agenzia per l'Italia Digitale, impongono l'adozione da parte degli Enti di un Piano di Disaster Recovery in grado di salvaguardare i servizi erogati mediante specifiche infrastrutture ICT.

La Continuità Operativa per la Pubblica Amministrazione rappresenta inoltre un'opportunità in quanto:

- Costituisce una componente essenziale dell'e-governement
- Consente agli Enti l'erogazione dei propri servizi con modalità sicure e affidabili
- Rappresenta un'occasione di analisi e miglioramento nella definizione e gestione delle infrastrutture ICT.

La Continuità Operativa, che estende la sua sfera di interesse alle tematiche più generali di natura organizzativa, considera gli strumenti tecnologici ICT impiegati nei procedimenti amministrativi come strumenti essenziali per l'erogazione dei servizi.

2.5 Obiettivi perseguiti

Prevenzione e gestione di eventi disastrosi con conseguenti risparmi indotti dalla mancata interruzione dell'erogazione di servizi. Possibile evoluzione tecnologica delle infrastrutture ICT dell'Ente con diminuzione dei costi operativi.

L'attuazione della normativa in materia di Continuità Operativa introdotta dal nuovo CAD, può diventare un'opportunità per il miglioramento dell'efficienza complessiva del funzionamento delle amministrazioni.

Per ottenere risultati coerenti ed in linea con la normativa, occorre procedere con un approccio commisurato alle caratteristiche della specifica amministrazione e alle esigenze dei servizi erogati, e soprattutto utilizzare metodologie di riferimento che consentano di raggiungere gli obiettivi definiti nelle "Linee guida per il Disaster Recovery della PA".

2.6 Azioni intraprese per la redazione della pratica

ND

2.7 Risultati raggiunti

Predisposizione dei seguenti servizi:

- **Condivisione di infrastrutture esistenti per la realizzazione di un CED secondario per *Disaster Recovery***

Disponibilità di spazi fisici attrezzati nel CED secondario per ospitare apparati server o di altra natura, dedicati a:

- Enti che non hanno un proprio CED ed intendono utilizzare l'infrastruttura del CED esterno per ospitare propri apparati
- Enti che pur avendo un proprio CED, si affidano al Consorzio per disporre del sito secondario a supporto del Piano di Disaster Recovery

- **Disaster Recovery di piattaforme virtuali**

Replica di piattaforme virtuali per Enti che dispongono di una infrastruttura di virtualizzazione VMware vSphere, HyperV, Xen Server destinato a Enti che erogano i propri servizi mediante un'infrastruttura ICT all'interno di un CED di proprietà, ovvero a Enti che, non disponendo di infrastrutture proprie, erogano i servizi avvalendosi di contratti di outsourcing con un fornitore esterno.

- **Disaster Recovery di piattaforme fisiche**

Replica dei dati e delle applicazioni nel Data Center secondario, per Enti che dispongono di una o più infrastrutture fisiche, di proprietà o nella disponibilità contrattuale, con le quali erogano i servizi.

2.8 Soggetti coinvolti nella redazione della pratica

La soluzione è stata sviluppata da CSI-Piemonte, Ente strumentale della Regione, al quale il Consiglio Regionale è consorziato.

2.9 Costi sostenuti per la predisposizione della pratica (IVA esclusa)

Unità di misura alternative:

- Euro (€)
- Costo totale della pratica **64.000,00** di cui:
- Interni: **0**
- Esterni: **64.000,00** , di canone annuo di infrastrutture ICT

Nota: I costi sostenuti sono riferiti alle attività necessarie per predisposizione della documentazione per l'acquisizione del parere dell'Agenzia per l'Italia Digitale, e dall'analisi BIA/RA necessaria per la realizzazione del Piano CO/DR. Sono inoltre comprese le attività professionali necessarie per la progettazione di dettaglio del modello organizzativo-procedurale e la redazione del Piano di Continuità Operativa, la progettazione di dettaglio delle soluzioni tecnologiche per il Disaster Recovery e la redazione delle relative procedure di attivazione.

I canoni annuali sono proporzionali alla complessità delle infrastrutture ICT del CED secondario a supporto del Piano di Disaster Recovery.

2.10 Finanziamento utilizzato

ND

3 MODALITÀ DI REALIZZAZIONE

3.1 Motivazioni che hanno portato alla implementazione della pratica

- Norma
- Regolamento

3.2 Modalità di implementazione della pratica

3.2.1 Durata di predisposizione della pratica: **9** mesi

3.2.2 Strumenti e/o modelli utilizzati per la predisposizione della pratica

ND