Il System Continuity Plan & la Business Continuity

Abstract

Obiettivo dell'attività di Business Continuity Planning è la realizzazione di un apparato organizzativo ed infrastrutturale che permetta ad un'azienda di assicurare il funzionamento ininterrotto dei propri processi critici a fronte di eventi potenzialmente dannosi. Tale attività viene documentata nel Business Continuity Plan.

Nell'ambito di questo complesso ed articolato processo la System Continuity è la parte più strettamente concernente i sistemi hardware e software posti a supporto dei processi aziendali.

Le modalità di realizzazione di un System Continuity Plan sono oggetto del presente articolo, che si prefigge di offrire una descrizione generale di questa importante attività.

Autori

Marco Giovinazzi, Ludovica Esposito (CISSP)
Security Competence Center (SCC) Roma, Bull

Indice

Introduzione

La Business Continuity è la capacità di mantenere costantemente disponibili i processi vitali e/o critici per l'azienda, a fronte di eventi potenzialmente catastrofici (disastri naturali, interventi umani dolosi e colposi, errori, etc.)

La pianificazione della continuità del business consente alle organizzazioni:

- di identificare gli impatti derivanti da eventuali interruzioni di servizio e perdite di dati;
- di formulare, implementare e mantenere piani di recupero per assicurare la disponibilità dei sistemi e delle applicazioni a supporto dei processi critici.

In tale ambito, la System Continuity ha il compito di assicurare la costante disponibilità delle applicazioni informatiche che nell'azienda sono poste a supporto dei processi di business ed il System Continuity Plan è lo strumento che consente all'azienda di ripristinare i sistemi hardware e sofware che consentono il funzionamento di tali applicazioni ("sistemi critici").

Nel seguito cercheremo di concentrare l'attenzione sull'attività di pianificazione della System Continuity, isolandola dal più ampio contesto della Business Continuity e descrivendone le fasi principali ed i risultati attesi.

La pianificazione della continuità dei sistemi

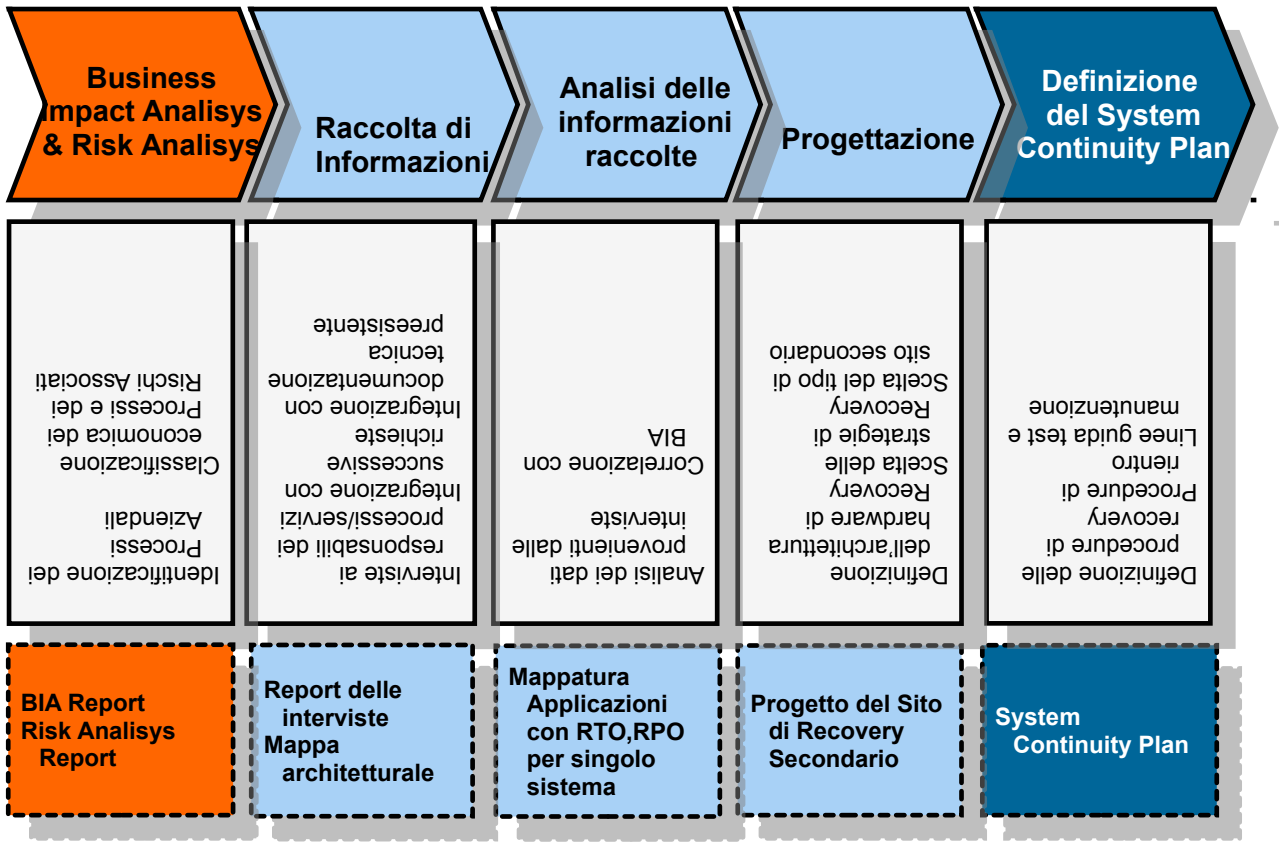

Fig.1: Schema delle attività principali

Prerequisiti: Business Impact Analysis & Risk Analysis

Una delle prime attività che vengono svolte durante la pianificazione della Business Continuity, è la Business Impact Analysis, il cui scopo consiste nell'identificazione e classificazione in temini di valore economico dei processi aziendali.

Il valore di ciascun processo/servizio viene stimato in base alle potenziali perdite economiche ("impatti") derivanti all'azienda dalla sua sospensione ed espresso in termini di tempo massimo durante il quale il processo/servizio può rimanere non funzionante prima che il danno alle operazioni di business divenga irreparabile.

I risultati di una business impact analysis costituiscono prerequisito per la fase di progettazione della soluzione di system continuity descritta nel seguito, poiché le relative scelte architetturali e tecnologiche sono vincolate dal valore di ciascun processo/servizio[1].

[1] Ciò perché i sistemi a supporto di processi che non possono cessare di funzionare neppure per un istante saranno ridondati con una spesa –e quindi una resa- assai maggiore rispetto ai sistemi coinvolti nel funzionamento di applicazioni che possono restare inattive per un paio di giorni!.

Un ulteriore importante prerequisito è costituito dall'analisi dei rischi associati agli impatti, che consente di determinare quali contromisure è ragionevole applicare in relazione alla probabilità di avvenire dei diversi eventi dannosi.

Fasi operative

Raccolta di informazioni

La prima fase operativa consiste in una raccolta di informazioni sufficienti a rispondere alle seguenti domande:

- Quali sono le applicazioni informatiche a supporto di ciascun processo/servizio?
- Quali sono (e come sono fatti!) i sistemi hardware necessari per far funzionare ciascuna applicazione?

Tali informazioni vengono raccolte per mezzo di una serie di interviste ai responsabili aziendali di ciascun processo/servizio.

Nell'ambito dell'intervista si deve cercare di individuare e descrivere in modo estremamente dettagliato tutti gli aspetti funzionali ed architetturali (configurazione, collegamenti, flussi da e verso sistemi esterni, etc..) che possono essere ritenuti rilevanti ai fini dell'attività si System Continuity.

Spesso l'intervista è seguita da una richiesta di chiarimenti relativi a particolari che non sono emersi durante il colloquio ed integrata con documentazione tecnica già presente in azienda.

Il team che conduce le interviste generalmente traduce tutte le informazioni raccolte in ciascun incontro in un report, che costituisce un utile strumento per rendere organico e memorizzare tutto ciò che è stato evidenziato.

Parte delle informazioni da raccogliere presenta valenza generale; si tratta di:

- Caratteristiche hardware
  - Tipo di CPU e frequenza
  - Memoria RAM
  - Quantità (in byte) di memoria di massa presente
  - Numero di HD, bus di collegamento e dati identificativi
  - Collegamento ad una Storage Area Network
  - Dispositivi di comunicazione, velocità degli stessi
- Caratteristiche Software
  - Sistema Operativo
  - Livello di aggiornamento/patch
  - Programmi accessori installati
  - ...
- Strategie di ripristino e backup (ove presenti)

- Responsabile/i del sistema
- Ubicazione del sistema
- Collegamenti verso sistemi esterni, velocità, tipo e flussi di dati stimati

Uno schema del genere sarà generalmente completato con ulteriori informazioni relative al particolare contesto, in modo che tutte le risorse utilizzate da ciascun processo/applicazione siano elencate e descritte (per esempio, se una stampante è ritenuta parte critica per il corretto funzionamento di un processo deve essere dettagliata sulla base delle sue caratteristiche, etc).

Spesso al termine della fase di raccolta è utile tradurre le informazioni in un'ampia e dettagliata mappa architetturale.

Analisi delle informazioni raccolte

In questa fase le informazioni raccolte mediante le interviste e quelle provenienti dalla BIA vengono opportunamente correlate, in modo da poter stabilire delle corrispondenze univoche tra il contesto applicativo (processo/applicazione, ciclo di vita, criticità, massimo tempo di inattività tollerata) e quello sistemistico (sistemi informatici coinvolti, siti, risorse utilizzate, etc.)

Per ciascuna applicazione individuata vengono definiti i valori di RPO (Recovery Point Objective, ovvero quanti dati è possibile perdere) ed RTO (Recovery Time Objective, ovvero quanto tempo l'applicazione può rimanere inattiva).

In base a questi valori si completa quanto rilevato nella fase precedente, circa le catene tecnologiche coinvolte nel ciclo di vita poichè gli stessi valori di RPO ed RTO dell'applicazione valgono anche per i relativi sistemi hardware.

In sintesi, al termine di questa fase di analisi, sarà noto per ciascuna applicazione,:

- di quali sistemi ha bisogno per funzionare ("mappatura delle applicazioni sulle catene tecnologiche");
- in quanto tempo si deve garantirne la ripartenza in caso di interruzione (RTO);
- quanti dati possono essere perduti in occasione dell'interruzione (RPO).

In questo modo è possibile realizzare il piano di System Continuity in base ad una scala "pratica" delle priorità (i sistemi posti a supporto dei processi che per l'azienda hanno maggior valore dovranno poter essere ripristinati più velocemente e con minor perdita di dati di quelli coinvolti in processi meno critici).

Raccolta di informazioni, analisi e presentazione dei risultati di entrambe queste fasi, vengono di solito effettuate con l'ausilio di metodologie standard che consentono un uso ottimale dei dati nel successivo passo, ovvero nella progettazione delle soluzioni di continuità.

Progettazione della soluzione di continuità

Questa fase ha come scopo la definizione di una soluzione che consenta di dare continuità al business dell'organizzazione secondo i requisiti raccolti ed analizzati, basata su di un'architettura hardware/software cost effective in grado di replicare tutte le catene tecnologiche vitali.

Poiché tra le possibili cause di grave interruzione sono presenti anche disastri di ampie proporzioni, che potrebbero rendere del tutto inagibili le sedi normalmente utilizzate per l'operatività dall'organizzazione, di norma tale soluzione prevede che tale architettura venga realizzata presso un sito dislocato in luogo geografico diverso da quello della sede abituale.

Per questo si parla di "sito di recovery" o "sito secondario".

La scelta del sito esula dagli scopi della System Continuity e rientra nel più ampio contesto delle attività di realizzazione del Business Continuity Plan. Vale la pena di ricordare, comunque, che l'area nella quale sarà create il sito secondario deve consentire l'agevole realizzazione di linee di trasmissione dati da/verso il sito (o i siti) primari e deve poter essere facilmente raggiunta dal personale tecnico addetto, in caso di interruzione dell'operatività nella sede principale.

Sebbene i requisiti dell'architettura di recovery siano ben chiari al termine della fase di analisi, la progettazione della soluzione è tuttaltro che semplice.

Partendo dalla lista delle applicazioni, mappate sui sistemi e corredate dei relativi valori di RPO/RTO, in questa fase si dovrà:

- Replicare l'architettura primaria senza omettere per ciascuna applicazione i collegamenti verso i sistemi esterni.
- Scegliere su quali componenti hardware/software replicare le applicazioni (cercando di ottimizzare le risorse e tenendo conto dell'ulteriore complicazione data dal fatto che spesso i sistemi primari non sono aggiornati rispetto al mercato delle tecnologie: sistemi operativi non più supportati, per esempio, costituiscono un inconveniente che emerge spesso in questa attività).
- Cercare di replicare i livelli di performance dei sistemi primari per garantire gli stessi livelli di servizio (o cercare di avvicinarsi ad essi quanto più possibile) laddove richiesto dal business.
- Progettare i collegamenti tra i sistemi primari e secondari per consentire che i dati siano presenti presso l'architettura secondaria nel rispetto dei requisiti di RPO/RTO.
- Rendere la soluzione completamente automatica, e minimizzare quindi la necessità di intervento umano per attuare e monitorare il passaggio da sistemi primari a secondari in caso di interruzione.
- Rendere il più possibile l'architettura di recovery espandibile e scalabile, per agevolarne il continuo ri-allineamento con quella primaria che si evolve secondo quanto imposto dalle esigenze di business dell'organizzazione. In tal senso potranno essere tenute in considerazione anche soluzioni tecnologicamente superiori alle primarie. Linee di trasmissione più veloci (ove possibile) di quelle presenti dovranno essere preferite, così come sistemi ad un livello di aggiornamento maggiore e che garantiscano supporto a lungo termine

mantenendo comunque la compatibilità all'indietro.

Per quanto riguarda la replica dei dati di produzione verso il sito secondario, nella progettazione si può scegliere tra due tipi di soluzioni precorribili:

- Replica periodica dei dati: i dati vengono periodicamente copiati sugli archivi del sito secondario in modo da minimizzare le differenze con quelli del sito primario. La scelta del tipo di backup varia dalla sovrascrittura completa, che richiede molto tempo e non è molto sicura (i dati sono continuamente in viaggio) al salvataggio incrementale/differenziale, più elastico e più sicuro, ma anche soggetto ad errori di disallineamento.
- Mirroring attivo del sito: tutte modifiche ai dati vengono effettuate di volta in volta sugli archivi primari e secondari, in modo da mantenere costantemente due copie identiche.

La differenza tra le due tecniche è sostanziale: la prima è sicuramente più conveniente dal punto di vista economico (non si devono predisporre linee dedicate sempre attive) e anche più veloce nel caso i dati vengano scritti in modo incrementale. La seconda invece è sicuramente più costosa ma anche più funzionale in caso di disastro, in quanto i dati sono sempre pronti per essere utilizzati e non c'è alcuna differenza tra archivi primari e secondari. C'è da dire però che, esclusi rari casi, la seconda strada è al limite della fattibilità e sicuramente sovradimensionata per la maggior parte dei requisisti di recovery che generalmente devono essere soddisfatti.

Spesso le organizzazioni scelgono di dare in outsourcing l'allestimento e la manutenzione del sito secondario; in tal caso, dal punto di vista dell'allestimento tecnologico, i siti vengono solitamente classificati come segue:

- Cold Site: è il tipo di sito meno costoso e di solito consiste in uno spazio di un edificio opportunemente dotato corrente elettrica e di rete dati. Tutto l'hardware necessario per la realizzazione dell'architettura di recovery deve essere portato all'interno del sito dopo che l'evento dannoso ha già avuto luogo. Naturalmente i cold site possono essere utilizzati solo per applicazioni con RTO molto elevati.
- Warm Site: contiene già l'hardware l'hardware necessario per la realizzazione dell'architettura di recovery. I dati sui sistemi devono essere aggiornati prima che le applicazioni possano essere lanciate e rese operative.
- Hot Site: contiene tutta l'infrastruttura hardware/software con la configurazione aggiornata; solo i dati devono essere allineati all'ultimo backup proveniente dai sistemi primari. Un hot site può essere portato in produzione in poche ore.
- Mirror Site: sito verso il quale i dati vengono replicati con tecniche di mirroring, molto veloci da rendere operativi.

Vale la pena a questo punto accennare al fatto che l'adozione di soluzioni virtualizzate, che permettono di "spostare" intere funzioni e risorse primarie, è in continua crescita. Virtualizzando le risorse, grazie all'adozione di software particolari, si rende una qualsiasi piattaforma hardware capace di svolgere molteplici funzioni e la velocità di messa in produzione di queste è quella di un semplice trasferimento di dati. Pur non essendo ancora tecnologie mature e soprattutto adatte a realtà di grandi dimensioni, questo tipo di soluzioni rappresenta un tema di sviluppo estremamente interessante per il prossimo futuro.

Il System Continuity Plan

Il System Continuity Plan è il documento che contiene gli elementi necessari per rendere operativa la soluzione di continuità dei sistemi in caso di interruzione della normale operatività di business.

Tra i principali elementi che esso deve contenere si trovano:

- il disegno architetturale del sito di recovery;
- le procedure che devono essere eseguite per rendere completamente operative le applicazioni nel sito secondario; naturalmente il piano sarà strutturato in modo da rendere operative per prime le applicazioni a supporto di processi di massima criticità, e a seguire quelle meno importanti (cioè partiranno per prime le applicazioni con valori più bassi di RTO)
- i riferimenti ai manuali tecnici specifici delle singole applicazioni.

Così come il Piano di Business Continuity contiene le procedure che devono essere eseguite perché l'intera organizzazione torni alla normale operatività presso la sede (le sedi) principale, anche il piano di System Continuity può contenere analoghe procedure più strettamente concernenti i sistemi informatici. Di solito nelle operazioni di rientro le prime applicazioni che vengono fatte ripartire sono quelle con criticità più bassa, al contrario di quanto avviene nella fase di recovery.

Il Piano può contenere le linee guida per i test periodici e la manutenzione della soluzione di continuità.

Conclusioni

La pianificazione della continuità dei sistemi è un obiettivo di vitale importanza per molte realtà aziendali nelle quali i processi fondamentali sono fortemente basati sull'uso di strumenti informatici. Il System Continuity Plan è lo strumento che consente di rendere operative le soluzioni scelte per dare continuità al business.

Le attività che vengono svolte per la redazione del Piano sono spesso occasione di ottimizzazione delle prestazioni dei sistemi informativi, oltreché di aumento della sicurezza delle informazioni e dello stesso business aziendale.

Gli elementi raccolti durante le fasi di indagine possono risultare utili anche al di fuori dell'ambito specifico del System Continuity Plan: la mappa architetturale che riassume quanto emerge dalle interviste ai responsabili dei processi/servizi, per esempio, è un documento spesso assente o non aggiornato, utilizzabile anche nellla più semplice ottica dell'assett management.