



Business Continuity: stato dell'arte

Intervento dell'ing. Anthony Cecil Wright –
Resp.le Sicurezza e Business Continuity - Banca Nazionale del
Lavoro e Presidente ANSSAIF

Contenuti della presentazione

- Dal Disaster Recovery alla Business Continuity.
- Cosa abbiamo imparato negli ultimi anni.
- Business Impact Analysis (BIA) e Risk Analysis.
- Esigenza di un Business Continuity Manager e suo posizionamento in azienda.
- Le indicazioni degli Enti preposti.
- Il progetto ABI-KPMG per un modello condiviso di Business Continuity Planning.

Antefatti: Dal D/R alla Business Continuity

- La tecnologia era limitata ed assai costosa.
- Le banche avevano (ed hanno tuttora!) obiettivi sempre più pressanti di riduzione dei costi.
- Le concentrazioni bancarie dovevano consentire sinergie e riduzione dei costi.
- Le probabilità di accadimento di eventi disastrosi erano quasi nulle.
- Pertanto, le soluzioni adottate minimizzavano i costi privilegiando polizze assicurative ed investimenti a protezione di eventi più probabili.

Antefatti: Dal D/R alla Business Continuity

- Le esperienze nel frattempo acquisite e, sopra ogni cosa, i noti eventi dell'11 settembre, hanno messo in crisi gli schemi citati.
 - Che una torre fosse distrutta, era ritenuta una fesseria.
 - Che entrambe le torri crollassero, una pazzia.
 - Che rimanessimo in Italia senza energia elettrica per più di un giorno, un' idiozia.
 - Che un incidente ad una delle centrali telefoniche di Roma, interrompesse i collegamenti nell'Italia Centrale, un'assurdità.
 - Ogni volta abbiamo detto: non era mai successo!
 - Mi domando e vi domando: "what next?".

Antefatti: Dal D/R alla Business Continuity

- Quanto dipendiamo oggi dall'automazione rispetto a soli due / tre anni fa?
- Le aziende di intermediazione finanziaria oramai trattano con i clienti mediante diversi canali di comunicazione: lo sportello, il cash dispenser, Internet, telefono... 24 ore al giorno per 7 giorni su 7. Oggi è richiesta alta disponibilità ed elevata velocità nella progettazione, nello sviluppo e nell'esecuzione.
- Allora, domandiamoci: ha senso di parlare di ripartenze in un giorno, e la perdita tra 24 e 72 ore di dati?
- Ma, anche: si può accettare una perdita di qualche ora di transazioni (in un grande gruppo, si parla di qualche milione di transazioni)? Oppure di assenza totale di informativa in tempo reale sull'andamento dei mercati?

Antefatti: Dal D/R alla Business Continuity

- La inglese FSA (Financial Services Authority) ha scritto nel suo documento "Financial Risk Outlook 2004":
 - (...) "Financial attacks could have both a physical and a market impact. So, the financial services industry needs to consider both physical resilience and its ability to deal with adverse market scenarios, while also remaining vigilant against being used for terrorist financing activities".
 - (...) "Firms will have to deal with a wave of legal, accounting and regulatory reforms".

La Business Continuity

- Da qualche anno a questa parte possiamo dire che esiste la tecnologia atta a permettere la dislocazione a forti distanze di una replica, anche sincrona, del patrimonio informativo di un'azienda o di un grande gruppo bancario.
- Ciò però ancora a costi estremamente elevati.
- E la nuova tecnologia, come vedremo più avanti, consente di ricoverare a forti distanze anche la "server farm" e, in generale, tutto il mondo "open".
- L'attenzione si è spostata dai CED all'intero gruppo aziendale, dal centro alla periferia.

La Business Continuity: BCP e BCM

- Le interrelazioni fra le procedure ed i processi aziendali ed interaziendali e la crescente complessità che deriva da quanto già detto, richiedono:
 - L'identificazione dei **processi vitali e critici** dell'azienda, incluse le interrelazioni con le controparti;
 - Un'analisi dell'**impatto** sui processi individuati derivante dall'eventuale verificarsi di un evento anche disastroso;
 - La **determinazione di due indicatori** importantissimi:
 - Il **tempo massimo di ripartenza** (Network Recovery Objective),
 - La **perdita massima** in termini di dati (Recovery Point Objective).

La Business Continuity

- I nuovi scenari hanno costretto le banche a porsi nuovi interrogativi: se dovessero venir meno il supporto informatico, quello informativo o quello logistico, quali sono i valori massimi accettabili di perdita dati e di tempo massimo di ripristino? Inoltre, quali perdite economiche progressivamente subirebbe l'azienda? E, purtroppo, da qualche tempo dobbiamo anche domandare ai responsabili delle unità organizzative: e se venissero meno delle persone "chiave"?

La Business Continuity

Consentitemi due parole sull'esperienza che abbiamo avuto a suo tempo in BNL e, in particolare, sulla Business Impact Analysis.

Un esempio: la BIA eseguita in BNL nel '02-'03

Ciò che più mi colpì, furono sia i risultati che emersero, con lo stupore degli stessi addetti ai lavori, sia il dialogo che conseguentemente si aprì.

La mia "lesson learned" fu:

- ***Utilizzare dati economici riscontrabili, dimostrabili;***
- ***Dedicare il dovuto tempo ai singoli passi:***
 - *alla stesura della scheda di rilevazione,*
 - *alla spiegazione degli obiettivi della rilevazione alle unità organizzative,*
 - *all'analisi congiunta delle informazioni fornite, e al loro confronto con altre fonti (ad esempio: controllo di gestione);*
 - *E, non ultimo, non affrettarsi, anche qualora si dovessero far slittare in avanti le scadenze inizialmente previste per la conclusione del progetto.*

Un esempio: la BIA eseguita in BNL nel '02-'03

Un'altra "lesson learned" fu che il dibattito si spostò successivamente molto più sulla prevenzione, che sulle misure di ripristino, con grande soddisfazione di tutte le parti. Non trascurabile, l'indirizzo verso progetti di razionalizzazione e consolidamento di ambienti.

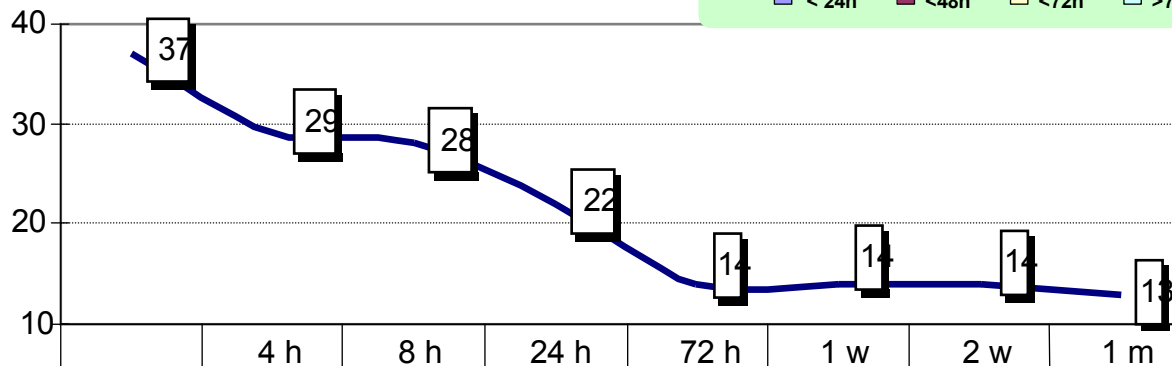
Oltre all'assoluta rilevanza ricoperta dal mondo "mainframe", emerse in tutta la sua portata la forte dipendenza dal mondo "open" e dalla informativa real-time (ad esempio: Reuters, Bloomberg, ecc.): decine di server di vario tipo (AIX, SUN, W/2K, ecc.), centinaia di postazioni e terabyte di dati! Anche per questo ambiente abbiamo trovato una soluzione che ha trovato tutti concordi.

(Mi fermo qui: MPS nella sua presentazione tratterà anche questi aspetti).

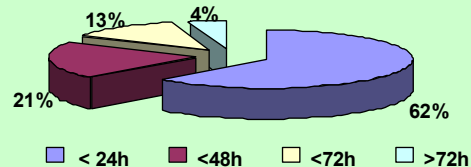
Esempio di un risultato della BIA

Grafico del Decadimento Processi Operativi

— N.Processi Attivi



Percentuale decadimento processi



N.Processi Attivi

37

29

28

22

14

14

14

13

4 h

8 h

24 h

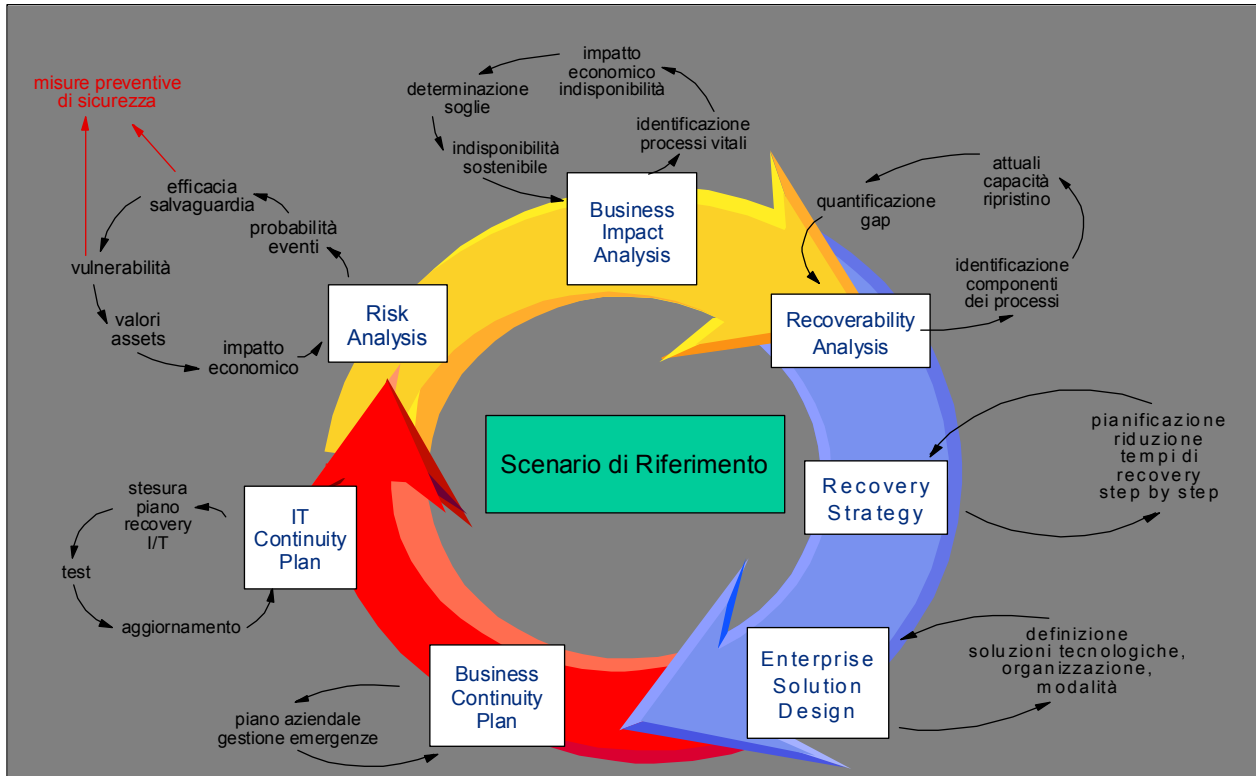
72 h

1 w

2 w

1 m

La metodologia utilizzata



La Business Continuity

- *Domande:*
 - ***quali sono i principali fattori di “facilitazione” di un così complesso processo di Business Continuity Planning (BCP)?***
 - ***Come coordinare le iniziative in un gruppo aziendale?***

Business Continuity: La bozza di linee guida sulla continuità operativa

- Banca d'Italia, nel mese di febbraio del 2003 invitò ad una riunione i principali intermediari finanziari e:
 - Illustrò le risultanze della ricognizione operata l'anno precedente sul sistema bancario;
 - Espose la bozza di linee guida per la continuità operativa che intendeva emanare;
 - Chiese a tutti e, in particolare all'ABI, di fornire indicazioni e commenti al riguardo.

Business Continuity: La bozza di linee guida sulla continuità operativa

- La Banca d'Italia ha innanzitutto fornito delle definizioni importanti:
 - La **gestione della continuità operativa** comprende tutte le iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti e catastrofi che colpiscono direttamente o indirettamente un'azienda.
 - Il **piano di continuità operativa**, anche denominato piano di emergenza, è il documento che formalizza i principi, fissa gli obiettivi e descrive le procedure per la gestione della continuità operativa dei processi aziendali critici.
 - Il **piano di disaster recovery** stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione dati. Il piano, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa.

La bozza di linee guida sulla continuità operativa: sintesi del contenuto

- La Banca d'Italia consegnò successivamente un'altra versione, a seguito delle risultanze sulla consultazione svoltasi presso il sistema finanziario.
- Le linee guida contengono indicazioni su:
 - Scenari da prendere in esame nella definizione del piano di continuità operativa per la gestione di situazioni critiche conseguenti ad incidenti di portata settoriale o catastrofi estese;
 - Correlazione ai rischi (operativi, reputazione, legali, credito, mercato, liquidità);
 - Definizione del piano e gestione dell'emergenza (**Ruolo dei vertici aziendali**; responsabilità del piano; contenuto; test; risorse umane; controlli interni; ecc.)
 - L'esigenza di definire requisiti particolari per le grandi banche.

La bozza di linee guida sulla continuità operativa: sintesi del contenuto

- Quali scenari:
 - Distruzione o inaccessibilità di una struttura nella quale sono allocate unità operative o apparecchiature critiche;
 - Indisponibilità di personale essenziale per il funzionamento dell'azienda;
 - Interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
 - Attacchi perpetrati dall'esterno attraverso reti telematiche;
 - Danneggiamenti gravi provocati da dipendenti infedeli.

La bozza di linee guida sulla continuità operativa (cont.)

- In particolare, sottolineo questi aspetti:
 - Sono introdotti scenari catastrofici anche estesi;
 - E' responsabilità del CdA stabilire obiettivi e strategie di continuità del servizio; assicurare risorse umane, tecnologiche e finanziarie adeguate; approvare il piano; venire informato, con frequenza almeno annuale, sulla adeguatezza dello stesso;
 - L'alta direzione deve nominare il **responsabile del piano di emergenza**; promuovere il controllo periodico del piano e l'aggiornamento dello stesso; approvare il piano annuale delle verifiche delle misure di continuità ed esaminare i risultati delle prove;
 - La responsabilità dello sviluppo, della manutenzione e dei test del piano di emergenza è affidata dall'alta direzione ad un esponente aziendale con posizione gerarchico-funzionale adeguata.

La bozza di linee guida sulla continuità operativa (cont.)

- Il piano di continuità deve documentare le modalità di dichiarazione dello stato di emergenza, l'organizzazione e le procedure da seguire in situazione di crisi, l'iter per la ripresa della normale operatività;
- I test si devono effettuare con frequenza almeno annuale, coinvolgendo gli utenti finali, gli outsourcer, e, se possibile, le controparti rilevanti;
- Porre attenzione alle risorse umane (lavoro in turni, addestramento, ecc.);
- Le verifiche sono correlate ai rischi;
- L'approccio alla continuità operativa e il piano di emergenza sono regolarmente verificati dalla funzione di revisione interna.

La bozza di linee guida sulla continuità operativa (cont.)

- Inoltre, vengono fissate delle indicazioni per gli intermediari ed operatori rilevanti (*ora scomparse dalla versione più recente, ma...*) quali:
 - i tempi massimi di ripristino delle attività critiche non devono superare le quattro ore dal momento dell'incidente;
 - va assicurata la chiusura contabile delle operazioni nella stessa giornata in cui si è verificato l'evento disastroso;
- Si forniscono altre utili raccomandazioni, fra le quali cito la necessità che la localizzazione dei siti sia adeguatamente distante e la ridondanza delle "utilities".

La bozza di linee guida sulla continuità operativa (cont.)

- In pratica, a mio avviso, la Banca d'Italia ha già dato una risposta ai precedenti interrogativi che ci eravamo posti; infatti:
 - Il **Vertice aziendale** è responsabile del **BCM** (dalla pianificazione, alla realizzazione, ai test, all'aggiornamento in base alle variazioni intervenute nei processi vitali o in aree che possano avere un impatto sugli stessi);
 - Deve essere nominato **un responsabile per il coordinamento delle attività** di BCP e BCM e deve essere di grado adeguato e posizionato opportunamente nella struttura gerarchica dell'azienda;

La bozza di linee guida sulla continuità operativa (cont.)

- Le **unità operative** coinvolte nei processi critici individuano i **responsabili di settore del piano di emergenza**. Essi coordinano, per gli aspetti di competenza, i lavori per la definizione del piano, per l'attuazione delle misure previste nello stesso e per la conduzione delle verifiche.
- Devono esistere **procedure formalizzate**;
- Deve esistere una **formazione continua del personale**;
- L'approccio alla continuità operativa e il piano di emergenza sono regolarmente controllati dalla funzione di revisione interna (**internal auditing**).
- La funzione di revisione interna è coinvolta nel controllo dei piani di emergenza degli outsourcers e dei fornitori critici. L'auditing controlla i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali.

La bozza di linee guida sulla continuità operativa (cont.)

- La Banca d'Italia è in procinto di emanare dette norme, ma, sulla base delle indicazioni in nostro possesso, prevedibilmente richiederà:
 - a tutto il sistema finanziario di eseguire le dovute analisi onde poter predisporre quanto prima i piani di Business Continuity, da attuarsi presumibilmente entro il 2007 (l'anno scorso lo richiedeva per il 2006);
 - agli operatori e intermediari di interesse sistemico, incontri individuali onde eventualmente imporre vincoli di ripartenza e ripristino più stringenti.

L'iniziativa ABI

- **Parallelamente, il C.E. dell'ABI autorizzava l'avvio di un progetto per la definizione di un modello condiviso di business continuity. Fu così costituito un Gruppo di Lavoro (GdL), composto dalle principali banche.**
- **Il GdL sulla Business Continuity scelse, dopo attenta valutazione, la Società KPMG Nolan & Norton per tale progetto.**
- **Lo scorso mese di gennaio, il GdL ha approvato il modello finale del documento "Metodologia di realizzazione del Piano di Continuità Operativa" e, se non erro, l'ABI l'ha già presentato alla Banca d'Italia.**
- **Chiaramente, il modello è coerente con le indicazioni della Banca d'Italia.**

Il Business Continuity Manager

- Abbiamo visto che la Banca d'Italia ha già espresso alcune importanti indicazioni.
- Che altre informazioni abbiamo?
- La già citata FSA, in Gran Bretagna, ha fatto una indagine presso un numero consistente di intermediari ponendo delle precise domande relativamente al processo di BCM al loro interno.
- In un rapporto ha riportato sia le conclusioni che il suo parere su quale deve essere la "best practice".
- Vi riporto alcune delle principali conclusioni.

La Business Continuity: il rapporto della FSA

Executive level accountability.

Si è riscontrato che ove vi era quale responsabile del BCM un membro del Consiglio ("Board"), si è riscontrata una maggiore sensibilizzazione e comprensione del BCM.

E' importante che il BCM continui ad essere sempre un problema del Consiglio e che l'intera organizzazione faccia propria la cultura del BCM e sposi appieno il processo di gestione della continuità. Il BCM deve essere trattato dal Consiglio almeno una volta l'anno.

La Business Continuity: il rapporto della FSA

BCM culture and awareness.

Si è purtroppo accertato che in molte aziende il processo di BCM rimane un processo di tipo "bottom-up", con un coinvolgimento non sempre chiaro del "senior management".

Ciò indica la difficoltà di avere il supporto del management.

Buona prassi è che il BCM sia affidato ad una funzione centrale, e che i rappresentanti delle business units siano responsabili sia dei singoli BCP sia di elevare la sensibilizzazione dei loro colleghi al BCM. Queste responsabilità degli incaricati di BCM nelle U.O. devono essere riportate negli obiettivi loro e delle rispettive U.O. di appartenenza. Loro è la responsabilità di produrre il BCP, che deve anche essere firmato dal responsabile della U.O.

La Business Continuity: il rapporto della FSA

BCM Function.

Mentre la funzione centrale di BCM è “chiave” per lo sviluppo di standard e metodi, è importante che essa abbia chiare responsabilità e linee di riporto.

E' buona pratica che la funzione centrale di BCM, non si limiti a monitorare la produzione dei piani delle U.O. e a partecipare nei test, ma deve anche verificare i piani, su base continua, per assicurarne la “consistenza” e completezza.

Per fare ciò detta funzione deve essere adeguatamente “staffata”.

La Business Continuity: il rapporto della FSA

BCM Budget.

Si è riscontrato che era uno standard l'esistenza di un budget centrale allocato alla funzione di BCM e per il costo dei siti di "contingency", mentre per il D/R dell'IT il budget era allocato a quella funzione.

Siccome molte aziende rivedevano il BCM dopo l'11 Settembre, è importante che siano assicurati adeguati fondi per la manutenzione e i test.

La Business Continuity: il rapporto della FSA

Altre indicazioni.

Non sto qui a riportare tutta la sintesi (diverse pagine).

Altre raccomandazioni sono relative a:

- Eccessiva vicinanza dei siti primario e secondario.
- L'identificazione delle minacce non era vista come una attività del risk management; in quelle aziende che includevano l'identificazione del rischio come parte della BIA, era buona pratica lavorare strettamente con l'Internal Audit e il Risk Management.
- E' di assoluta importanza creare gruppi differenziati di gestione dell'emergenza e della crisi; ossia team strategici, tattici, locali. Questi gruppi intervengono in base alla natura dell'evento.
- Porre grande attenzione agli accordi con le terze parti e, se del caso, rivederli in modo da assicurare di avere, all'occorrenza, quanto necessario per riprendere rapidamente l'attività. (...)

La Business Continuity: il FFIEC

- Un'altra citazione: il Federal Financial Institutions Examination Council ha prodotto un booklet sul *Business Continuity Planning* per gli Enti che devono esaminare le aziende di intermediazione finanziaria.
- Oltre a ribadire quanto già sostenuto dalla Banca d'Italia e dalla FSA, è interessante notare che in tale documento insiste più di una volta che un BCP non è da considerare valido se non è stato certificato da una terza parte indipendente ed è stato provato.

La Business Continuity: un costo elevato

- A bassi tempi di ripristino e a quasi nulla perdita di dati, corrispondono, lo sappiamo, **costi sempre più elevati** sia per investimenti che per spese ricorrenti.
- Vi è quindi necessità di un **bilanciamento** attento, ma soprattutto condiviso da tutto il management, fra **costi e benefici**.
- Si devono pertanto prendere in esame:
 - i possibili scenari di rischio e le conseguenze sui processi,
 - l'efficacia delle azioni preventive esistenti,
 - le misure di emergenza attualmente previste;
 - si deve misurare il **rischio residuo**, e, quindi, individuare i costi delle possibili ulteriori misure preventive, di ripristino e di emergenza da adottare.

La Business Continuity: un costo elevato

- La BC è solo un costo?
- Interessante, a questo proposito, un articolo pubblicato su un documento prodotto congiuntamente dalla British Bankers' Association e dalla KPMG e dal titolo "The link between BCM and economic capital".
- In estrema sintesi, si sostiene – opportunamente documentandolo - che gli impegni in BCM dovrebbero essere dedotti dal capitale allocato non solo ai fini del rischio operativo, ma anche di quelli di business, credito e mercato.

La Business Continuity: un costo elevato

- In un recente incontro con la Banca d'Italia si è anche affrontato il problema dei grossi investimenti richiesti dai progetti in corso e da quelli necessari agli operatori ed intermediari di interesse sistemico.

Se ho compreso bene, le banche centrali hanno già sottoposto l'argomento all'attenzione del Comitato di Basilea; non sono esclusi anche ulteriori passi verso altre sedi istituzionali.

In conclusione abbiamo esaminato:

✓ Dal Disaster Recovery alla Business Continuity.

In conclusione abbiamo esaminato:

- ✓ Dal Disaster Recovery alla Business Continuity.
- ✓ Cosa abbiamo imparato negli ultimi anni.

In conclusione abbiamo esaminato:

- ✓ Dal Disaster Recovery alla Business Continuity.
- ✓ Cosa abbiamo imparato negli ultimi anni.
- ✓ Business Impact Analysis (BIA) e Risk Analysis.

In conclusione abbiamo esaminato:

- ✓ Dal Disaster Recovery alla Business Continuity.
- ✓ Cosa abbiamo imparato negli ultimi anni.
- ✓ Business Impact Analysis (BIA) e Risk Analysis.
- ✓ Esigenza di un Business Continuity Manager e suo posizionamento in azienda.

In conclusione abbiamo esaminato:

- ✓ Dal Disaster Recovery alla Business Continuity.
- ✓ Cosa abbiamo imparato negli ultimi anni.
- ✓ Business Impact Analysis (BIA) e Risk Analysis.
- ✓ Esigenza di un Business Continuity Manager e suo posizionamento in azienda.
- ✓ Le indicazioni degli Enti preposti.

In conclusione abbiamo esaminato:

- ✓ Dal Disaster Recovery alla Business Continuity.
- ✓ Cosa abbiamo imparato negli ultimi anni.
- ✓ Business Impact Analysis (BIA) e Risk Analysis.
- ✓ Esigenza di un Business Continuity Manager e suo posizionamento in azienda.
- ✓ Le indicazioni degli Enti preposti.
- ✓ Il progetto ABI-KPMG per un modello condiviso di Business Continuity Planning.

The end