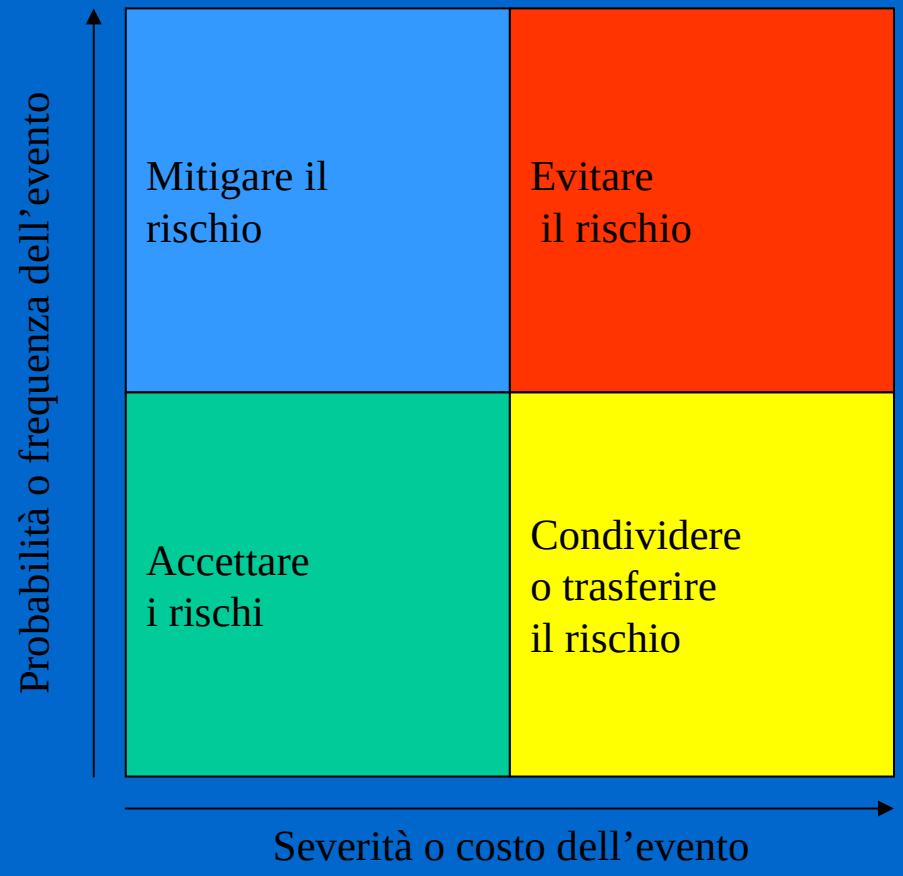
Agenda

- **La Continuità Operativa nella Pubblica Amministrazione Italiana: esigenze operative e infrastrutture critiche nazionali**

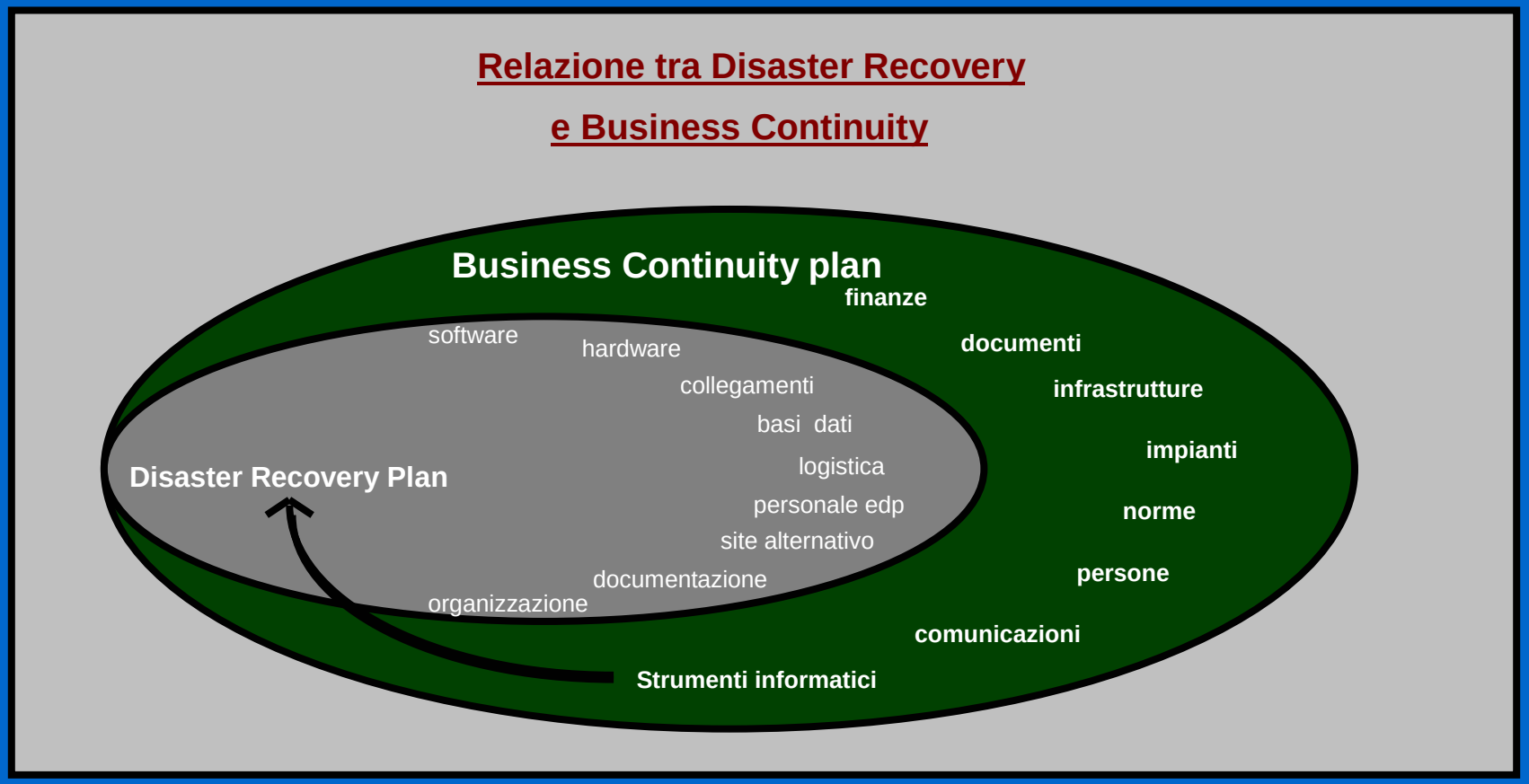
- **Le Linee Guida per la Continuità Operativa**

La Continuità Operativa nella Pubblica Amministrazione Italiana: esigenze operative e infrastrutture critiche nazionali

La logica di trattamento dei problemi di sicurezza



Business continuity e Disaster recovery in letteratura



La continuità operativa nel settore pubblico

- La continuità operativa si propone di trattare in modo unitario qualunque problema di discontinuità del servizio che assuma rilevanza per durata e dannosità
- Alcune soluzioni di continuità operativa permettono di affrontare anche problemi di natura ordinaria (fermi contenuti o programmati)
- La pubblica amministrazione è tenuta ad assicurare la continuità dei propri servizi per garantire il corretto svolgimento della vita nel Paese (si ricorda l'art. 97 della Costituzione ed il principio di buon andamento dell'amministrazione, da rispettare anche se si utilizzano tecnologie ICT)

Norme in materia di continuità operativa

- Direttiva del 16 gennaio 2002
- Codice in materia di protezione dei dati personali
  (Decreto legislativo 30 giugno 2003, n. 196)
- Codice dell'amministrazione digitale
  (Decreto legislativo 7 marzo 2005, n. 82)
- D.P.C.M. 31 maggio 2005
  (Gazz. Uff. 18 giugno 2005, n. 140)
- Legge 24 dicembre 2007, n. 244 (Finanziaria 2008)
  (Gazz. Uff. 28 dicembre 2007, n. 300)

Norme in materia di continuità operativa

Direttiva del 16 gennaio 2002

- La Direttiva recante "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali", del 16 gennaio 2002, pubblicata sulla G.U. n. 69 del 22 marzo 2002 sollecita le pubbliche amministrazioni a porre attenzione ai temi della sicurezza, valutando i rischi e attuando contromisure in grado di contenerne probabilità e conseguenze:

"Sicurezza nelle tecnologie dell'informazione e della comunicazione

Le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese. Questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse. E' noto infatti che esistono minacce di intrusione e possibilità di divulgazione non autorizzata di informazioni, nonché di interruzione e di distruzione del servizio."

Norme in materia di continuità operativa

Codice in materia di protezione dei dati personali
(Decreto legislativo 30 giugno 2003, n. 196)

- Articolo 31: I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i **rischi di distruzione o perdita, anche accidentale**, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

- Misure minime: adozione di procedure per la custodia di copie di sicurezza, il **ripristino della disponibilità dei dati e dei sistemi**

Norme in materia di continuità operativa

Codice dell'amministrazione digitale

(Decreto legislativo 7 marzo 2005, n. 82)

- Art. 2, comma 1. Lo Stato, le Regioni e le autonomie locali **assicurano** … **la fruibilità dell'informazione in modalità digitale** e si organizzano ed agiscono a tale fine …
- Art. 3 (Diritto all'uso delle tecnologie). I cittadini e le imprese hanno **diritto a richiedere ed ottenere l'uso delle tecnologie** dell'informazione e della comunicazione **nei rapporti con le pubbliche amministrazioni** centrali e con i gestori di pubblici servizi statali …
- Art. 4 (**Partecipazione al procedimento amministrativo** informatico) …
- Art. 5 (**Effettuazione dei pagamenti** con modalità informatiche) …
- Art. 6 (**Utilizzo della posta elettronica certificata**) …
- …
- Art. 12: Le pubbliche amministrazioni … utilizzano le tecnologie dell'informazione … **obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione**
- Art. 15: La **riorganizzazione strutturale e gestionale** delle pubbliche amministrazioni … avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione ….
- Art. 51 (**Sicurezza dei dati**):
  - 1. Le norme di sicurezza … garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.
  - 2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati … ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito …

Razionalizzazione in merito all'uso delle applicazioni informatiche

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 di cui all'art. 1 del decreto legislativo 12 febbraio 1993, n. 39, anche con l'introduzione di nuove tecnologie e servizi.*

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.".

Finanziaria 2008

(Legge 24 dicembre 2007, n. 244, GU n. 300 del 28 dicembre 2007 - Supplemento ordinario n. 285)

Art 2 commi 582- 583

- 582. *Al fine di salvaguardare e di garantire l'integrità, anche ai sensi dell'articolo 51 del citato codice di cui al decreto legislativo 7 marzo 2005, n. 82, e delle disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, del patrimonio informativo gestito dalle amministrazioni pubbliche di cui all'articolo 1 del decreto legislativo 12 febbraio 1993, n. 39, e al fine di garantire la disponibilità e la continuità dei servizi erogati dalle stesse amministrazioni, il CNIPA identifica idonee soluzioni tecniche e funzionali riguardanti, in generale, diverse amministrazioni, atte a garantire la salvaguardia dei dati e delle applicazioni informatiche nonché la continuità operativa dei servizi informatici e telematici, anche in caso di disastri e di situazioni di emergenza.*

- 583. *Il CNIPA, ai fini dell'identificazione delle soluzioni di cui al comma 582, indice conferenze di servizi.*

Infrastrutture Critiche

- Lo sviluppo, la sicurezza e la qualità della vita nei paesi industrializzati dipendono dal funzionamento continuo e coordinato di un insieme di infrastrutture che, per la loro importanza e strategicità, sono definite Infrastrutture Critiche. Queste includono tutti quei servizi essenziali per il benessere della popolazione, la sicurezza nazionale, il buon funzionamento del Paese e la sua crescita economica. Vale a dire il sistema elettrico ed energetico, le varie reti di comunicazione, le reti e le infrastrutture di trasporto persone e merci (aereo, navale, ferroviario e stradale), il sistema sanitario, i circuiti economico - finanziari, le reti a supporto del Governo, delle Regioni ed enti locali, quelle per la gestione delle emergenze, ecc..

- La "*Direttiva sull'identificazione e designazione delle Infrastrutture Critiche Europee e sulla verifica della necessità di migliorare la loro protezione*" dell'Unione Europea giunge come conclusione di un iter normativo avviato dalla richiesta, da parte del Consiglio Europeo, La Direttiva si articola su alcuni concetti chiave:
  - Individuazione delle ICE
  - Punto di Contatto mediante un organismo nazionale competente per la protezione delle Infrastrutture Critiche.
  - Valutazione dei rischi
  - Piani di Sicurezza dell'Operatore
  - Funzionario di collegamento

Le attività del CNIPA per la Continuità Operativa

- *L'organizzazione*:
- *Sezione Continuità operativa nell'ambito dell' Area "Indirizzo, supporto e verifica P.A.C."*
  - *Gruppo di Lavoro*
  - *Comitato Direttivo e segreteria tecnica del CUB*

Le attività del CNIPA per la Continuità Operativa – Centro Unico di Backup

- **Attività per il Centro Unico di Backup:** Il Centro unico di backup è un progetto esteso agli enti previdenziali ed assicurativi con la sottoscrizione di un protocollo d'intesa tra Cnipa, Inps, Inail, Inpdap, Ipost. Il CNIPA svolge le seguenti funzioni:
  - Segreteria Tecnica
  - Predisposizione di test collettivi
  - Predisposizione di atti e attività per la prosecuzione del centro comune.

Le attività del CNIPA per la Continuità Operativa- Supporto alle Amministrazioni

Il supporto alle Amministrazioni prevede:

- I pareri specifici per la Continuità Operativa.
- Lo sviluppo di uno strumento di autovalutazione
- Consulenze
- La predisposizione di modelli di Piani di Continuità Operativa
- La predisposizione di documenti sul tema, quali linee guida, casi di studio, ecc.

Lo strumento di autovalutazione

- Lo strumento di autovalutazione consente di misurare le esigenze di Continuità Operativa delle Amministrazioni. Partendo dalla classificazione delle Amministrazioni, in base alle esigenze di CO ed ai parametri citati nelle linee guida, lo strumento di autovalutazione consente di individuare l'appartenenza alle classificazioni rispetto alle possibili soluzioni di CO. In particolare lo strumento valuta i seguenti parametri:
- **Tipologia e caratteristiche dell'amministrazione**:
  - Numero di dipendenti;
  - Numero di sedi;
  - Bacino di utenza, sia in termini di cittadini, che di imprese;
  - Vincoli normativi
  - Presenza di dati sensibili nelle banche dati.
- **Caratteristiche del Sito primario**:
  - Spese sostenute per l'IT, annue;
  - Potenza elaborativa;
  - Numero e tipologia di server applicativi;
  - Gestione della infrastruttura IT;
  - Numero di siti dotati di infrastruttura IT;
  - Numero di siti IT con accesso alle risorse consentito anche a personale non esplicitamente autorizzato.
- **Caratteristiche dei servizi IT offerti**:
  - Percentuale dei servizi interattivi, sul totale offerto;
  - Periodo di offerta dei servizi;
  - Periodicità dei picchi di richiesta;
  - Numero di interruzioni dei servizi in un anno tollerabili dall'amministrazione;
  - Numero di interruzioni dei servizi in un anno tollerabili dall'utenza;
  - Cause degli ultimi fermi di servizio e relativi effetti sulla collettività (p.e. perdita di fiducia).
- **Definizione dei Ruoli nei processi di recupero operativo**:
  - Presenza di una definizione formale dei ruoli chiave da contattare durante il processo di ripristino;
  - Esistenza di procedure di emergenza;
  - Esistenza di sistemi di backup.

Le Linee Guida per la Continuità Operativa

Struttura delle Linee Guida

1. Aspetti metodologici

2. Analisi costi benefici

3. Organizzazione delle strutture di gestione della Continuità operativa

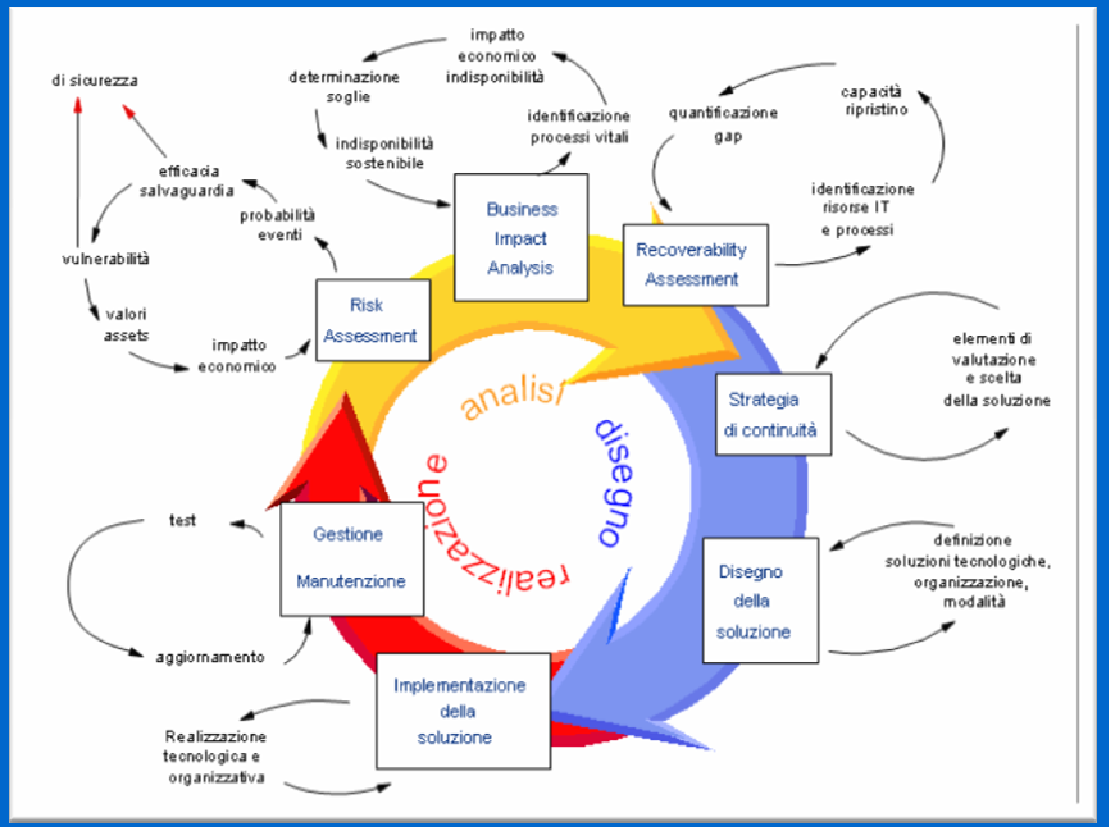
4. Strumenti giuridici per l'acquisizione di un servizio di continuità

5. Tecnologie per la continuità operativa

Aspetti metodologici 1/3

- Il termine "metodologia" indica un insieme strutturato di attività che, condotte in un dato ordine, definiscono un percorso che porta a un obiettivo prefissato.
- In questa sezione viene trattata la scelta della soluzione principalmente sotto l'aspetto tecnico-organizzativo.

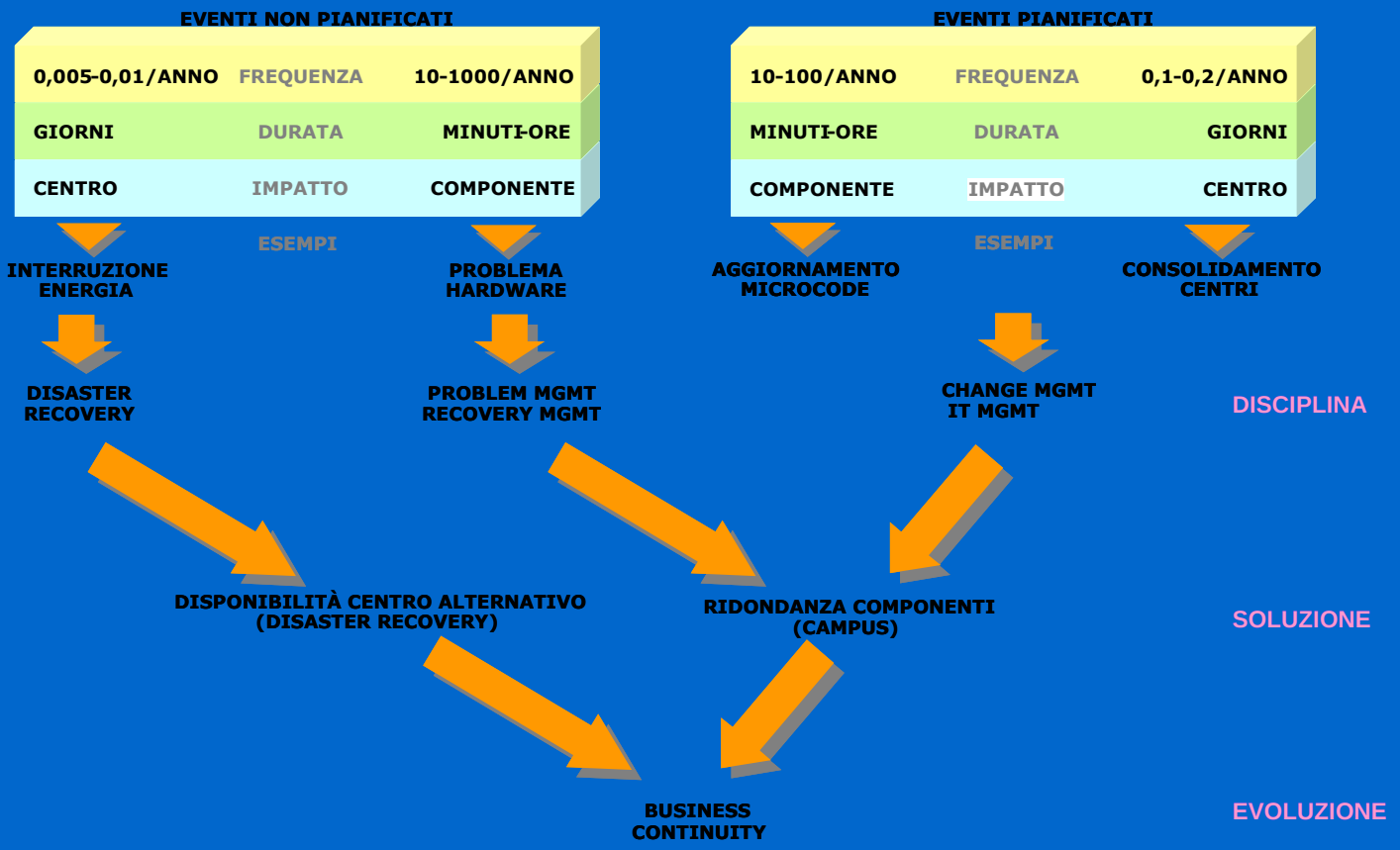
- le fasi metodologiche sono:
  - la fase iniziale di studio/analisi del contesto,
  - disegno della soluzione tecnologica e organizzativa che meglio risponde alle esigenze di continuità richieste,
  - realizzazione e mantenimento della soluzione.



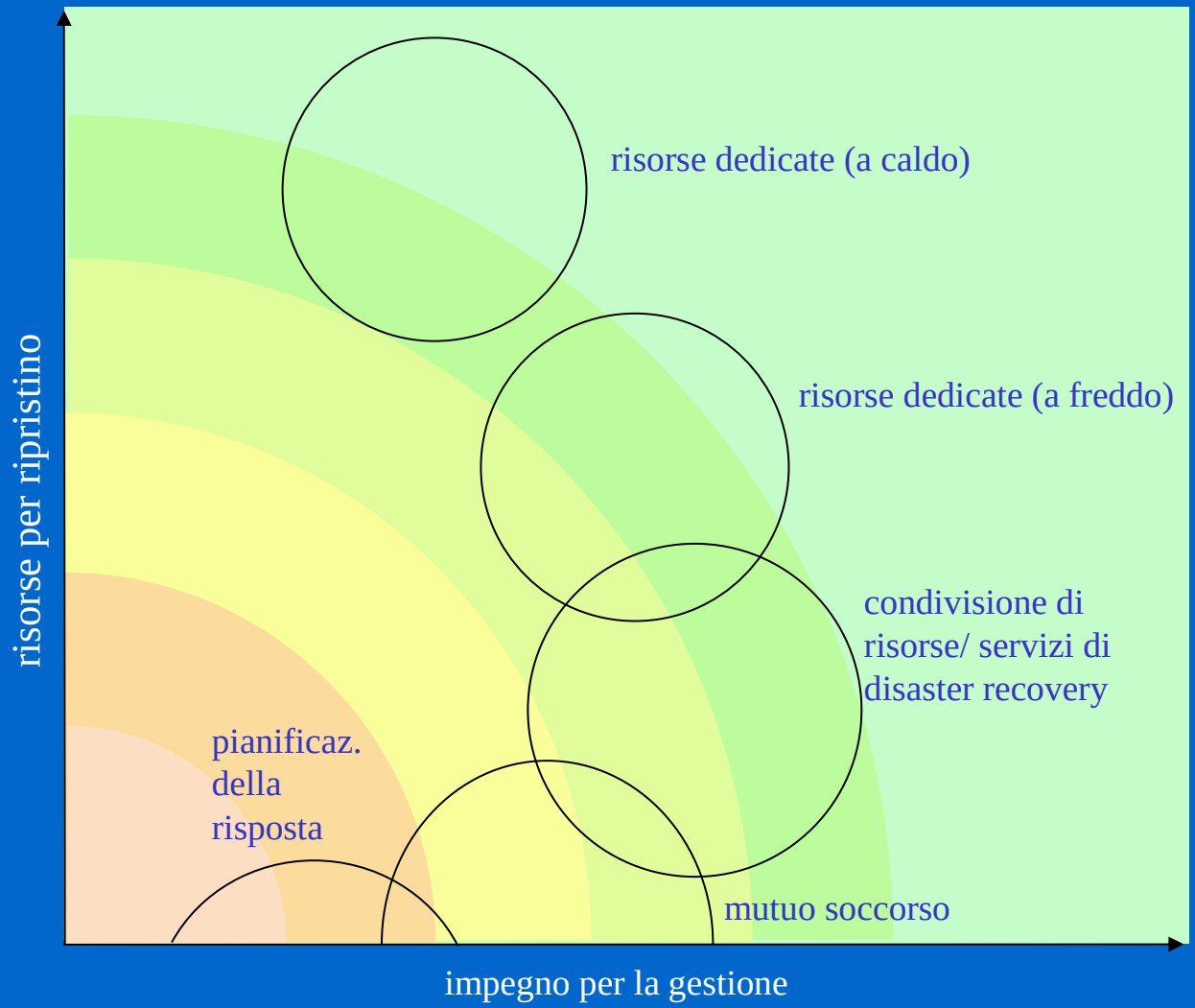
Aspetti metodologici 2/3

- Tutti i percorsi metodologici esistenti hanno come punto di partenza lo **studio del contesto di riferimento** , cioè del quadro tecnologico e organizzativo all'interno del quale esiste un' esigenza di continuità operativa da soddisfare.
- Lo studio del contesto è indirizzato a stabilire la tipologia di eventi dalla quale l'amministrazione intende proteggersi:
- Gli eventi vengono identificati in :
  - eventi pianificati (es.: manutenzione degli impianti tecnologici, aggiornamento di componenti, lavori di ristrutturazione della sede, ecc...);
  - eventi non pianificati (incidenti, guasti all'alimentazione elettrica, cadute della rete, malfunzionamenti, ecc …), in grado di causare indisponibilità prolungata dei servizi

Aspetti metodologici 3/3



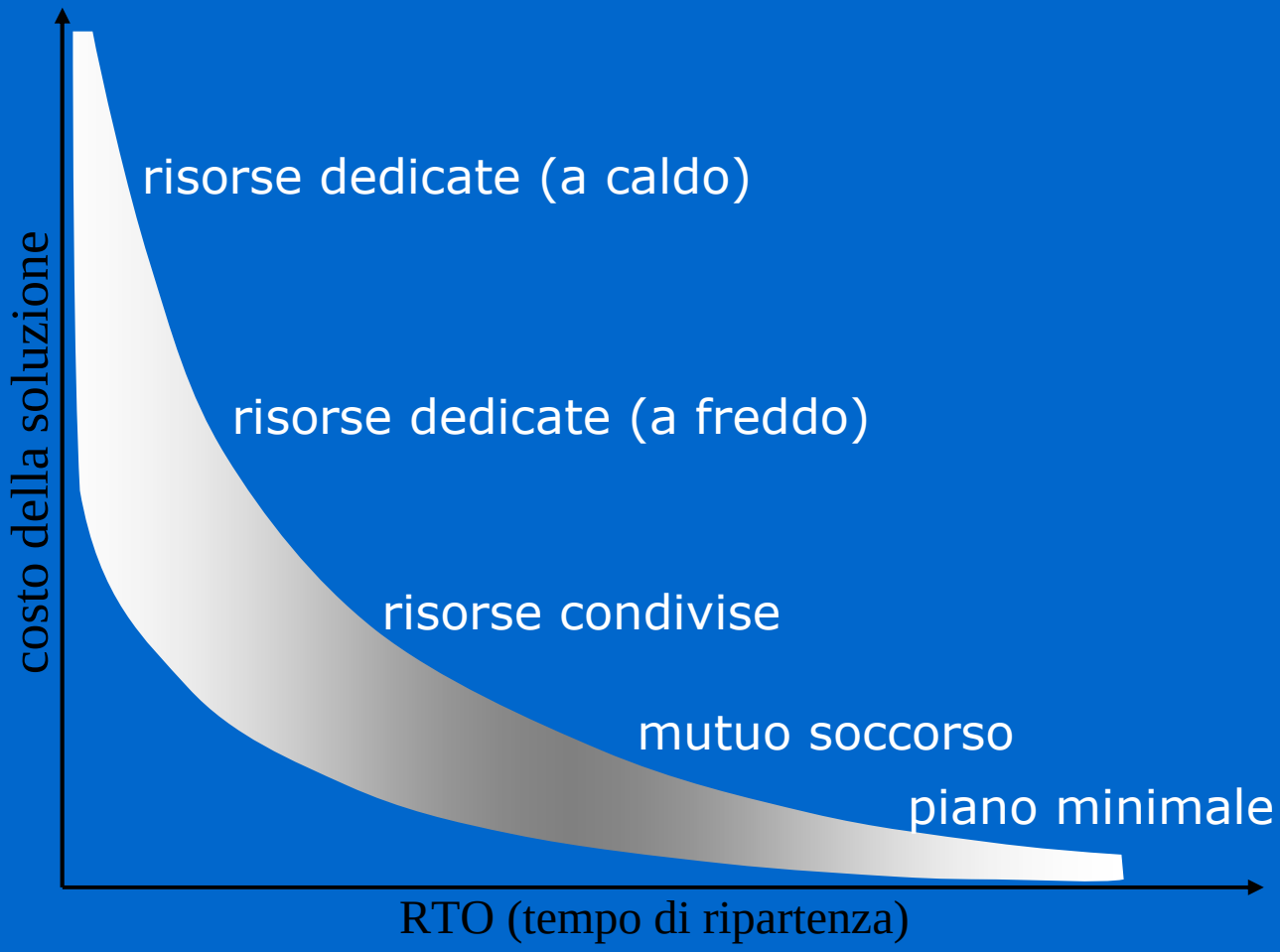
Risorse per la gestione e per il ripristino



Soluzioni idonee per classe di amministrazione

	Tipologia di amministrazione			
	Classe A	**Classe B**	**Classe C**	**Classe D**
Mutuo soccorso	x	x		
Risorse condivise	x	x	x	
Risorse dedicate (a freddo)		x	x	x
Risorse dedicate (a caldo)			x	x
Adeguamento procedure salvataggio dati	x	x	x	x
Consolidamento o razionalizzazione		x	x	x
Aumento della resilienza		x	x	x
Servizi di disaster recovery	x	x		
Accordi per fornitura apparati	x			

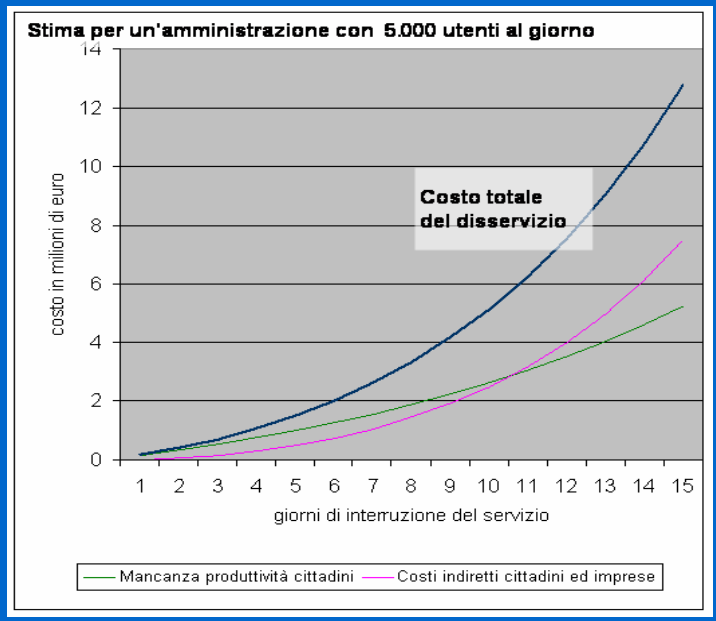
Relazione tra costo e tempo di ripartenza



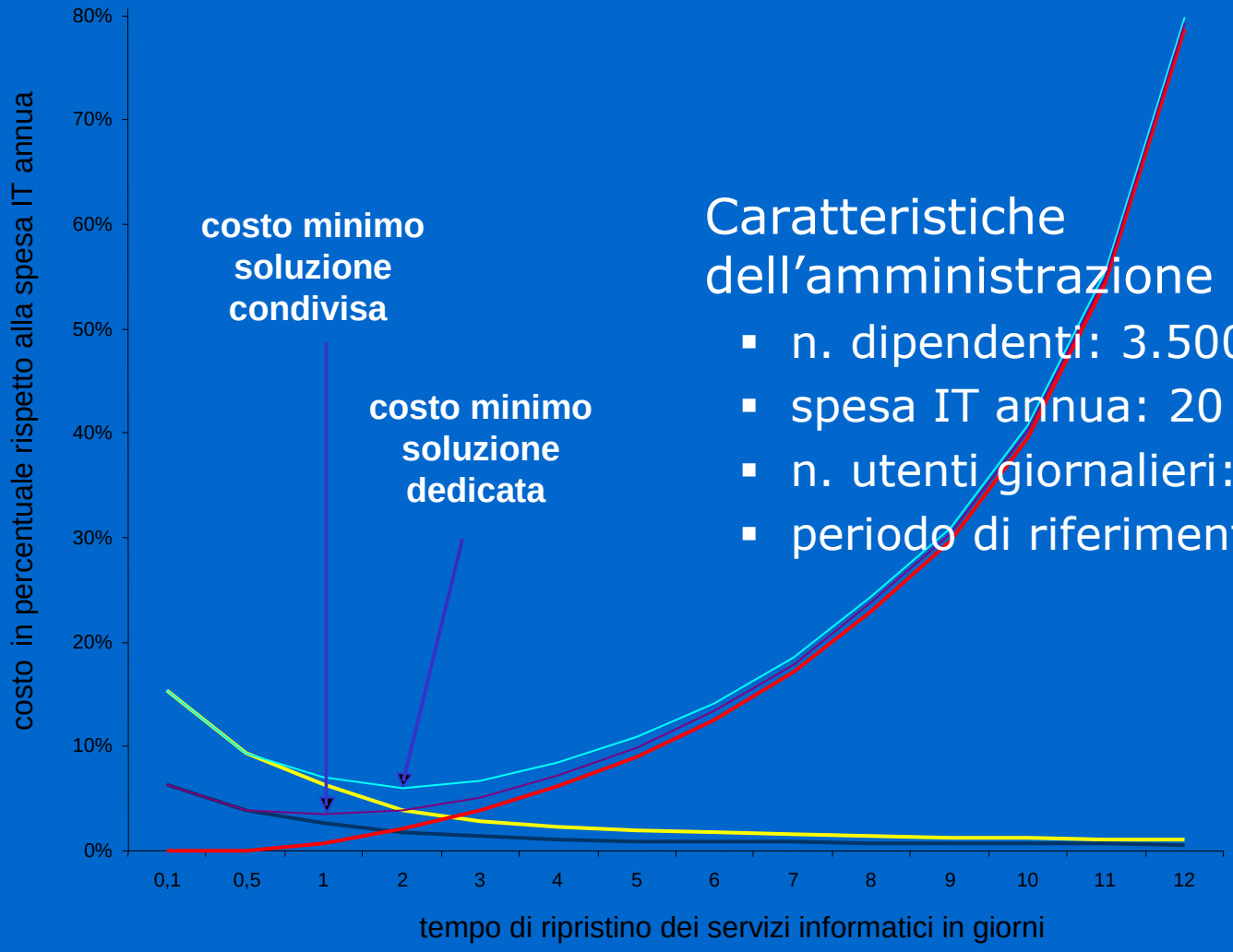
Analisi costi/benefici

- L'analisi dei costi e dei benefici delle soluzioni inizia sin dalla fase di studio del contesto ed è effettuata, in particolare, nel corso della business impact analysis. L'analisi economica si sviluppa, poi, durante l'esame delle soluzioni possibili.
- L'analisi economica ha come obiettivo la scelta del miglior compromesso tra costi da sostenere per la realizzazione della soluzione e costi generati dalla assenza di servizio.
- Il metodo di analisi economica proposto si basa sul confronto tra i costi delle diverse soluzioni ammissibili ed i costi che l'amministrazione deve sostenere in caso di evento che provoca l'interruzione dei servizi, costi che saranno diversi a seconda della soluzione di continuità operativa attivata. In generale, più costosa è la soluzione di continuità scelta (e migliori le sue caratteristiche in termini, ad esempio, di RTO e RPO), più limitati saranno i danni economici derivanti dall'interruzione del servizio

Esempio di valutazione dell' andamento
del costo per collettività derivante dall'interruzione
dei servizi resi da un'amministrazione di grosse dimensioni.
Si è ipotizzato che i servizi vengano utilizzati quotidianamente da circa 5.000 utenti



Un esempio



Caratteristiche dell'amministrazione

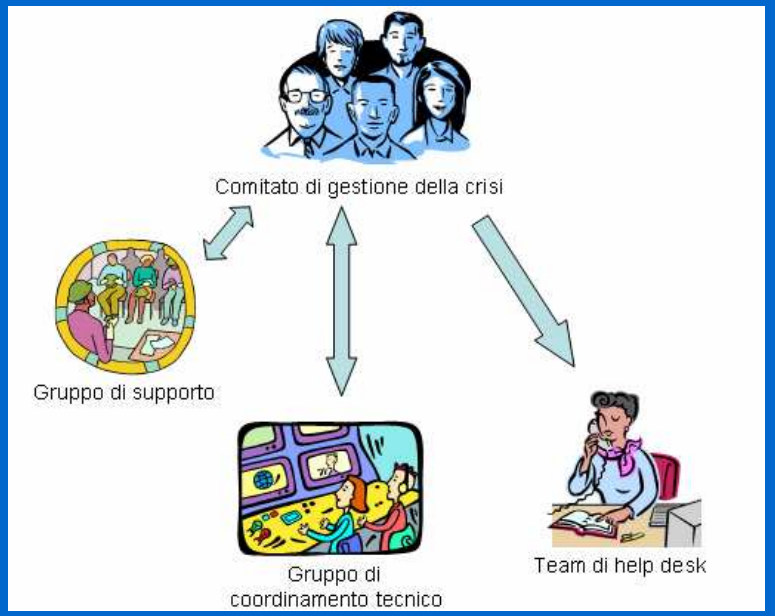
- n. dipendenti: 3.500
- spesa IT annua: 20 M€
- n. utenti giornalieri: 5.000
- periodo di riferimento: 4 anni

Benefici per l'Amministrazione

- La realizzazione di una soluzione di continuità operativa comporta diversi benefici poiché richiede attività di rilevazione ed inquadramento dei procedimenti che sono molto utili per la razionalizzazione e l'ammodernamento dei processi e dell'amministrazione.
  - Vantaggi per la revisione ed ottimizzazione dell'architettura attraverso i processi di consolidamento.
  - interventi architetturali sono molteplici e vanno dalla riduzione della spesa informatica al miglioramento dei livelli di servizio.
  - Vantaggi per l'organizzazione della continuità operativa poiché prevede la creazione di strutture e di relazioni finalizzate alla gestione dell'emergenza. Queste relazioni, consolidate attraverso le prove periodiche, di solito sono utili anche in situazioni di emergenza non necessariamente correlate a problemi di continuità operativa. Permettendo di affrontare meglio anche altri problemi di sicurezza.
  - Vantaggi nella creazione di un sistema alternativo dedicato, consente attività di manutenzione ordinaria, incrementando significativamente il livello di disponibilità dei servizi informatici.

Organizzazione delle strutture di gestione della Continuità operativa

- Questa sezione propone consigli e indicazioni per la creazione delle strutture incaricate di gestire le problematiche della continuità su come creare e organizzare, all'interno di una amministrazione pubblica
- La struttura organizzativa preposta a gestire le problematiche di continuità operativa all'interno di un'amministrazione ha per definizione la missione di:
  - predisporre tutte le misure necessarie per ridurre l'impatto di un'emergenza;
  - valutare la portata dell'evento e la sua effettiva gravità;
  - scegliere se innescare o meno i processi definiti per il ripristino.
  - mettere a disposizione risorse alternative a quelle non disponibili;
  - governare il sistema durante l'emergenza;
  - gestire il rientro alla normalità.



E' opportuno che la struttura organizzativa definita per la continuità abbia responsabilità e compiti ben definiti, e che possieda ampia autonomia decisionale e disponibilità di utilizzare risorse straordinarie.

Comitato di Gestione Crisi

- Il Comitato di gestione della crisi è un organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività degli altri gruppi. E' l'organo di direzione strategica dell'intera struttura, e ha inoltre responsabilità di garanzia e controllo sull'intero progetto.

- I suoi compiti principali sono:
  - approvazione del piano di continuità operativa;
  - valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi;
  - avvio delle attività di recupero e controllo del loro svolgimento;
  - rapporti con l'esterno e comunicazioni ai dipendenti;
  - attivazione del processo di rientro;
  - avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
  - dichiarazione di rientro;
  - gestione di tutte le situazioni non contemplate;
  - gestione dei rapporti interni e risoluzione dei conflitti di competenza;
  - promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità.

Strumenti giuridici per l'acquisizione di un servizio di continuità

- Direttiva del 16 gennaio 2002
  - Articolo 34:"… f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;"
- Codice dell'amministrazione digitale (Decreto legislativo 7 marzo 2005, n. 82)
  - art. 51 (Sicurezza dei dati), comma 2: "I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta."
- D.P.C.M. 31 maggio 2005 (Gazz. Uff. 18 giugno 2005, n. 140)
  - Art. 3, lettera 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."
- Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)
- D.P.C.M. 6 agosto 1997, n. 452 (Gazz. Uff. 30 dicembre 1997, n. 302)

Tecnologie per la continuità operativa

- Backup dei dati
  - nastri magnetici LTO
  - nastri virtuali
  - backup remoto
  - replica dei dati
  - Copia locale e replica fuori linea
  - replica in linea
  - replica logica
- I collegamenti in rete
  - affidabilità della rete
  - continuità delle reti locali
  - continuità delle reti IP
- La virtualizzazione dei dati
  - metodi di connessione dei dispositivi di memorizzazione
  - le SAN (Storage Area Netvork)
  - tecniche per la virtualizzazione
- Tecnologie per il sito di emergenza
  - hot standby
  - cluster remoto

Il backup

- Le copie di backup devono essere conservate in luoghi “sicuri”
- La tecnica deve essere scelta tenendo conto del requisito RPO
- I metodi si dividono in
  - fuori linea
  - in linea
    - sincroni
    - asincroni

La rete

- Due diverse esigenze
  - *affidabilità della rete*
    - superamento dei limiti di distanza per le connessioni in geografico
    - protocolli per il recupero della connettività nelle reti locali
    - re-instradamento automatico a seguito di caduta di un nodo (protocolli di livello 3)
  - *collegamenti in emergenza verso i sistemi di backup*

La virtualizzazione

- Virtualizzazione dei dati
  - Storage Area Network
  - Disaccoppiamento tra applicazioni e sistema aziendale di gestione dei dati
- Virtualizzazione dei processi
  - Web services
  - Grid computing