ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Le soluzioni di protezione dati per la continuità dei servizi IT e la Security Compliance in ambito bancario

Ing. Chiara Benvenuti
Ing. Carlo Fragale

Roma, 3/7/2012

Agenda

- Introduzione alla Business Continuity e al Disaster Recovery
- Analisi del Contesto e degli Scenari di Disastro
- Disaster Recovery – Organizzazione e Documentazione
- La Continuità Operativa per le PP.AA.
- La Continuità Operativa in ambito bancario
- Q&A

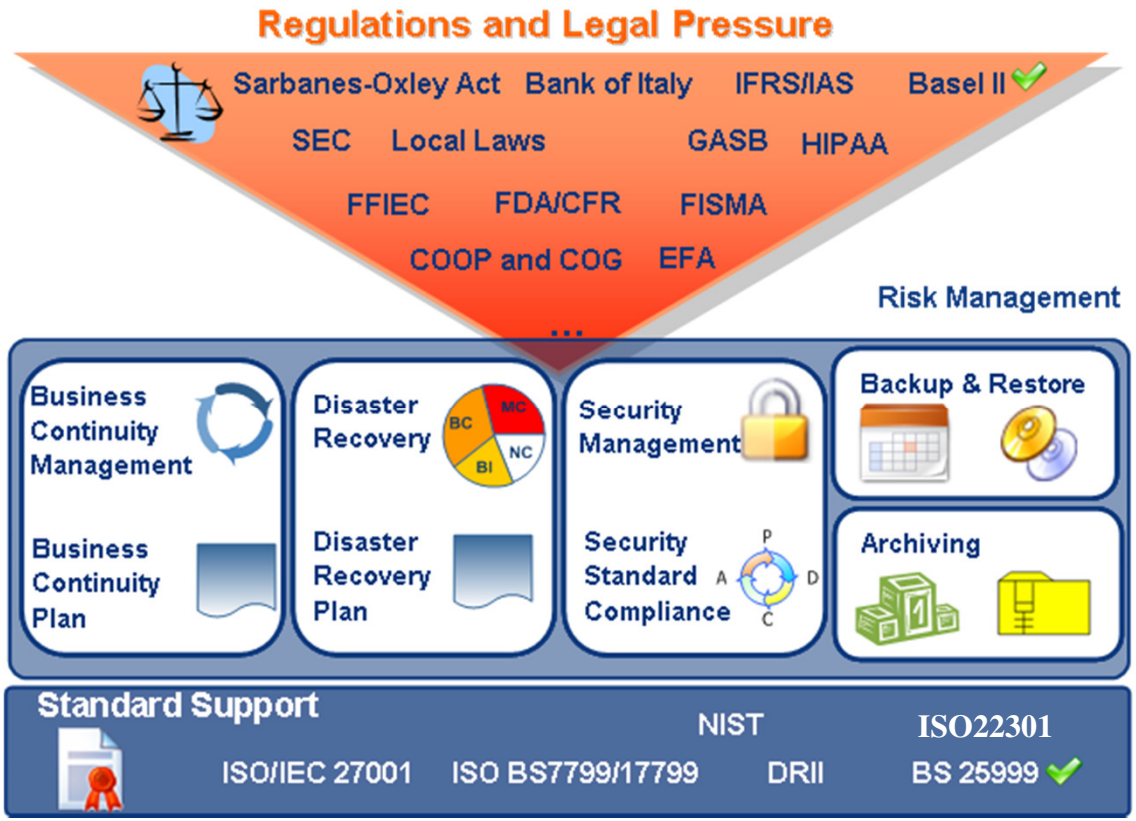
Business Continuity e Disaster Recovery

Business Continuity Management è un processo strategico e tattico che permette ad un'organizzazione di avere una risposta a qualunque avvenimento e interruzione del Business che può avere impatto sui processi aziendali che contribuiscono al “core business” dell'azienda, garantendo un livello di servizio minimo accettabile predefinito.

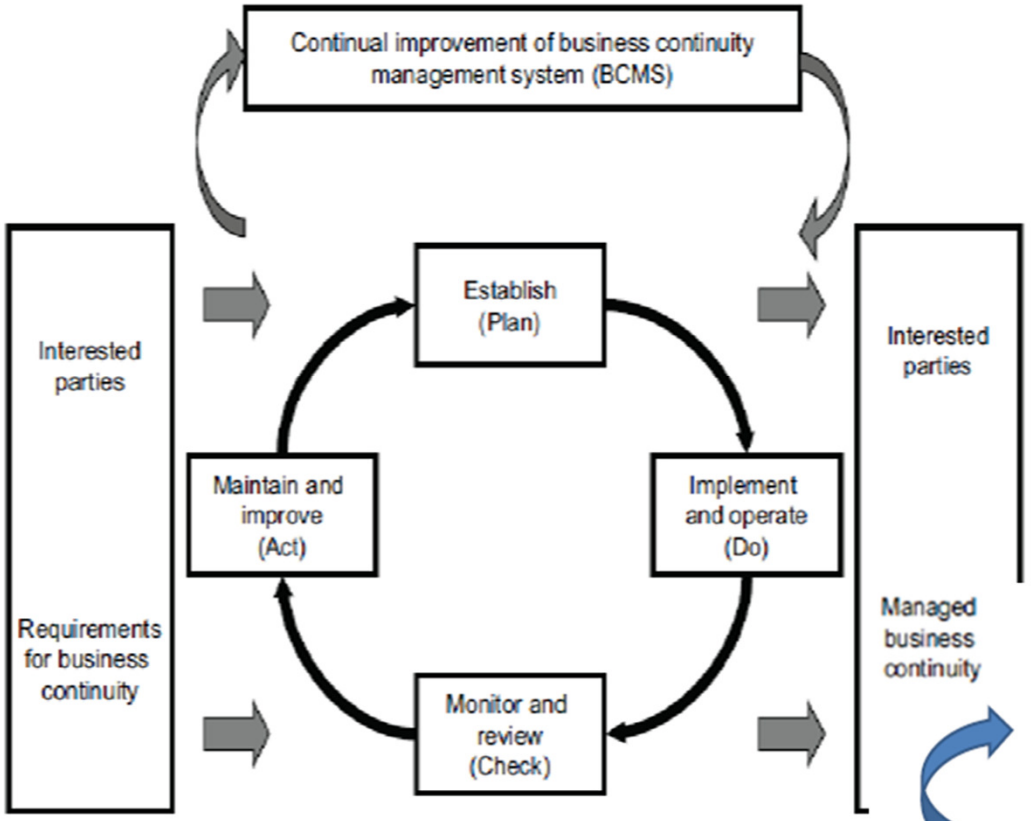
Disaster Recovery è l'insieme di processi e tecnologie atti a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi “core business” a fronte di gravi emergenze (disastri).

Perchè Business Continuity e Disaster Recovery?

La Business Continuity aiuta le aziende nel proteggere il loro business e nell'ottenere la compliance con le leggi internazionali e le regolazioni, riducendo i rischi e migliorando il rapporto prestazioni/costi.



Approccio metodologico – ISO22301



- Nuovo Standard ISO (International Organization for Standardization) 22301 per la gestione della continuità operativa.
- Deriva dallo standard BS25999 di BSI (British standards Institution)

Il Disaster Recovery

Quale **Danno al Business Aziendale** può derivare dall'indisponibilità prolungata delle **Applicazioni** e/o dalla perdita dei **Dati Aziendali?**

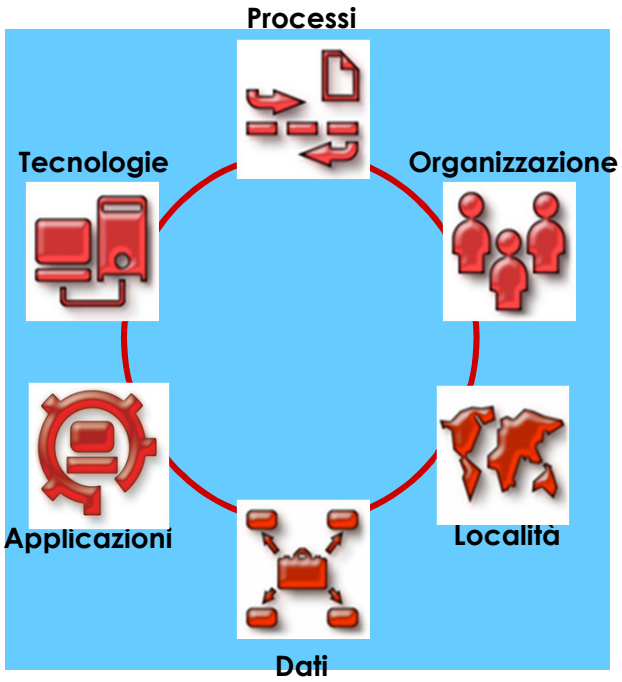
Il **Disaster Recovery (DR)** è l'insieme di…

…**Tecnologie** e **Processi** predisposti per ripristinare le …

…**Applicazioni** e i **Dati** necessari all'erogazione dei…

… **Servizi di Business**, interrotti a seguito di…

…**Gravi Eventi Dannosi** (**Disastri**).



Perchè il Disaster Recovery?

- Limitare le perdite dovute a riduzione di revenue o ad altri costi
- Minimizzare l'interruzione di Processi Business Critical
- Soddisfare ai requisiti imposti da obblighi di compliance
- Evitare di compromettere la reputazione e la solidità della azienda
- Definire dei processi semplificati di decisione e di azione per fronteggiare una situazione imprevista
- Preservare le business operations e "sopravvivere" in caso di possibili failures
- Prevedere un ritorno "controllato" alla normale operatività

Prepararsi al Disaster Recovery

Presupposti per rispondere efficientemente ad una situazione di emergenza:

- **Criteri** per riconoscere una **Condizione di "Disastro"** e attivare le **Politiche d'Intervento**
- **Conoscenza** della **Criticità** dei **Dati**, delle **Applicazioni** e la loro **Priorità**
- **Obiettivi Misurabili** per il **Ripristino del Servizio**

Prepararsi al Disaster Recovery

- **Valutare** il potenziale **danno al business** derivante dall'indisponibilità prolungata delle **Applicazioni** e/o dei **Dati Aziendali**.
- **Pianificare** contromisure tecnologiche e organizzative per prevenire o gestire le **Emergenze**
- **Progettare** risorse e processi per prevenire e fronteggiare le emergenze
- **Implementare** sistemi e procedure operative di supporto
- **Eseguire** le procedure operative ordinarie di custodia dei **Dati** e della **Configurazione**
- **Verificare** periodicamente e sistematicamente l'efficacia e l'efficienza di tutte le procedure di gestione delle emergenze
- **Intervenire** sulle **Non-Conformità**
- **Pianificare** il miglioramento continuo dell'intero sistema

Prepararsi al Disaster Recovery

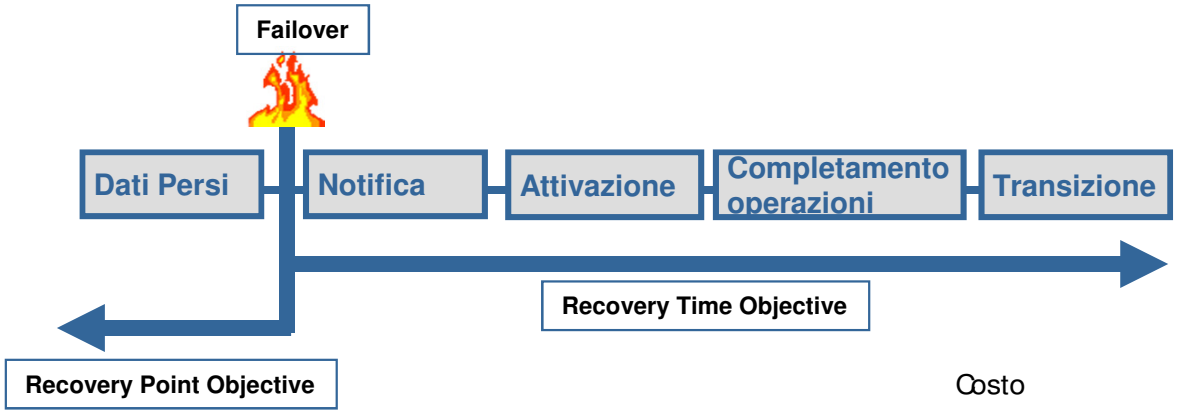
- Non è un intervento “una tantum” ma un **Processo Operativo/Gestionale** continuo

- Non è un **Lusso** ma una **Necessità** per l’Azienda

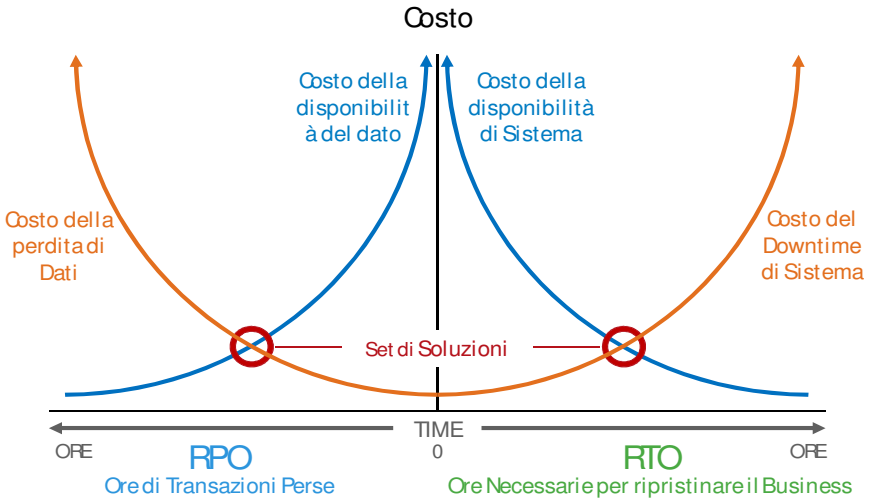
I Livelli di Servizio

I requisiti di Business si traducono in requisiti Tecnologici, le cui metriche sono:

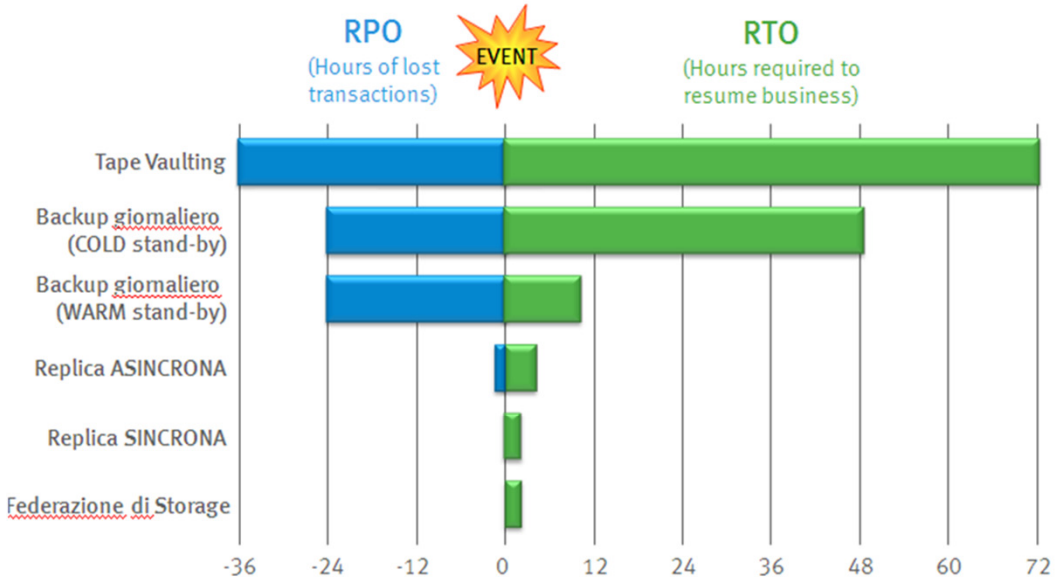
- **RTO** (Recovery Time Objective) = esprime in ore, l'intervallo temporale ammissibile di indisponibilità dei sistemi in seguito ad un disastro.
- **RPO** (Recovery Point Objective) = esprime in ore, l'ammontare massimo di dati che possono essere persi in seguito ad un disastro.

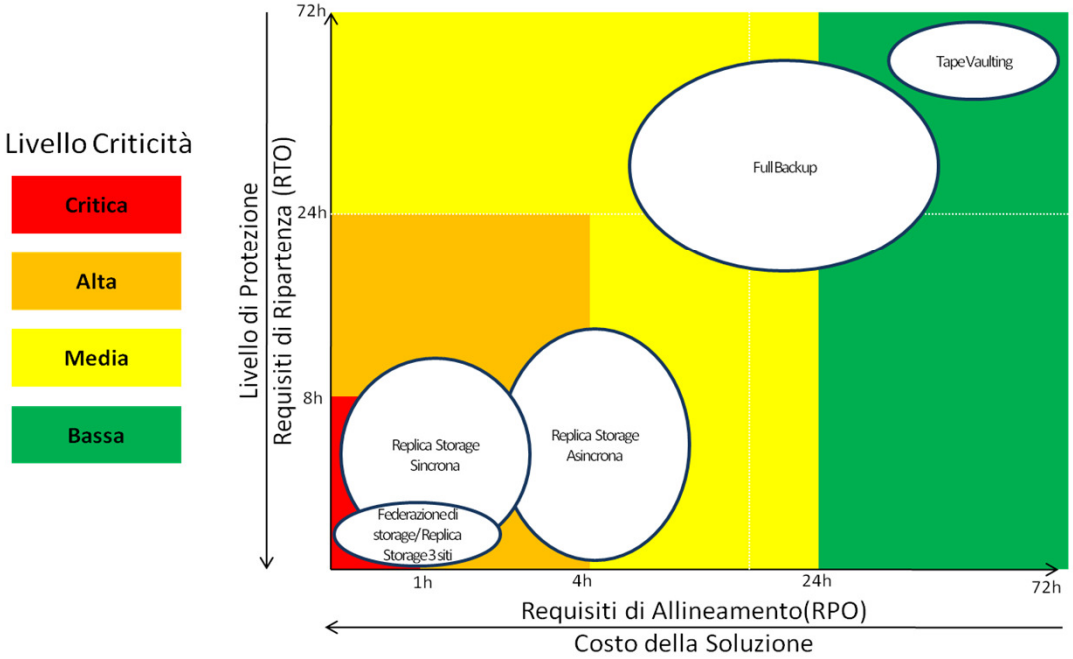


L'ottimizzazione dei parametri di RTO e RPO dipende dal compromesso tra i costi dovuti alla perdita di dati e dai costi di implementazione di una architettura di DR efficiente (in figura una rappresentazione grafica).



Tecnologie e Livelli di Servizio





Agenda

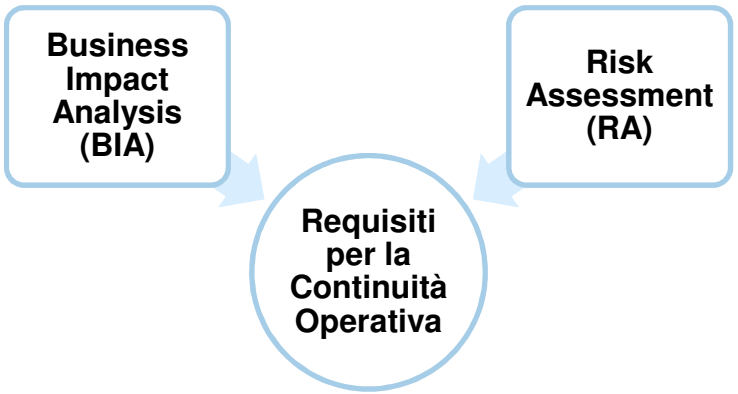
- Introduzione alla Business Continuity e al Disaster Recovery
- Analisi del Contesto e degli Scenari di Disastro
- Disaster Recovery – Organizzazione e Documentazione
- La Continuità Operativa per le PP.AA.
- La Continuità Operativa in ambito bancario
- Q&A

Analisi del Contesto

Per “Analisi del Contesto” si intendono tutti quegli studi e quelle attività volti ad indagare l’ambiente oggetto di Continuità Operativa, al fine di determinarne le esigenze ed i requisiti di protezione.

In tal senso, attraverso l’analisi del Contesto tipicamente si studiano:

- la realtà oggetto di Continuità Operativa (imprese, PP.AA)
    - •asset (tra cui il personale)
    - •organizzazione
    - •obiettivi e missione
    - •politiche, processi e meccanismi di sicurezza,
- gli ambienti operativi (processi, servizi, applicazioni) e le tecnologie a supporto



Analisi del contesto – BIA (1/2)

DEFINIZIONE

Studio delle caratteristiche e delle esigenze aziendali finalizzato a determinare l'importanza e la criticità dei processi e dei servizi in termini di business.

La metodologia della BIA consente di valutare le conseguenze derivanti dal verificarsi di un evento critico e di valutarne l'impatto in termini operativi o monetari.

STANDARD

- DigitPA – Linee Guida
- NIST SP 800-34
- BS 25999/ISO 22301

METODOLOGIA

Analisi del contesto – BIA (2/2)

DIMENSIONI DI IMPATTO (tipiche)

- *Aspetti economico-finanziari*
- *Aspetti reputazionali (immagine)*
- *Aspetti normativo-legali*
- *Aspetti di competitività commerciale*

OUTPUT

- *Classificazione Processi*
- *Classificazione Risorse*
- *Impatti (Processo →Servizio →Risorsa)*
- *Caratterizzazione Servizi*
- *Livelli Servizio (RTO, RPO)*

Analisi del contesto – RA (1/4)

DEFINIZIONE

Insieme delle attività finalizzate a determinare una classificazione dei rischi aziendali relativamente alle minacce applicabili.

I rischi vengono classificati attraverso un algoritmo che prende i considerazione:

- Probabilità di accadimento delle minacce
- Conseguenze derivanti dall'esposizione degli asset alle minacce (livelli di impatto)
- Grado di esposizione alle minacce degli asset
- Livello di vulnerabilità degli asset

Il legame tra BIA e RA viene ben riportato dalla definizione che DigitPA fornisce del Risk Assessment:

"...analisi per determinare il valore dei rischi di accadimento di un evento che possa interrompere la continuità operativa" valutando "sul patrimonio informativo che supporta i processi critici dell'Amministrazione il valore di rischio in rapporto alla probabilità di accadimento di un evento (o minaccia), al suo grado di esposizione (vulnerabilità) ed in funzione dell'impatto determinato nella fase di BIA" e declinando "gli scenari di rischio che potrebbero [...] produrre danni rilevanti all'Amministrazione secondo quanto stimato nella BIA."

STANDARD

- ISO-IEC 27005
- ISO-IEC 31000
- NIST SP 800-30

Analisi del contesto – RA (2/4)

Livello di Rischio = Probabilità accadimento minaccia x Impatto sull'Asset
Livello di Rischio Residuo = Livello di Rischio a valle dell'adozione delle azioni di trattamento del rischio (ad es. Contromisure)

RA Qualitativo

- Metodologia di Analisi del Rischio in cui tutti i fattori ed i parametri oggetto di indagine (probabilità di accadimento delle minacce, livello di vulnerabilità, impatto di una minaccia su di un asset, livello di rischio, ...) vengono stimati in valori discreti non numerici/economici
- Le stime vengono effettuate tipicamente su base esperienza, attraverso interviste, brainstorming, workshop, ...
- Una metodologia che consente di minimizzare la soggettività delle valutazioni è quella detta "di Delphi", attraverso la quale un board di esperti fornisce proprie opinioni/stime assieme alle relative motivazioni; attraverso un meccanismo di feedback iterato su più "round", una figura di "facilitatore" modera il processo che conduce alla convergenza delle stime dei diversi esperti.
- Il livello di rischio è espresso attraverso livelli discreti (es: alto, medio, basso)

RA Quantitativo

- Metodologia di Analisi del Rischio che assegna ai fattori ed ai parametri in oggetto valori numerici ed economici.
- Il livello di rischio è un valore numerico pari allla perdita economica associata allo scenario di disastro indagato.
- Una tipica formula di calcolo del Rischio:

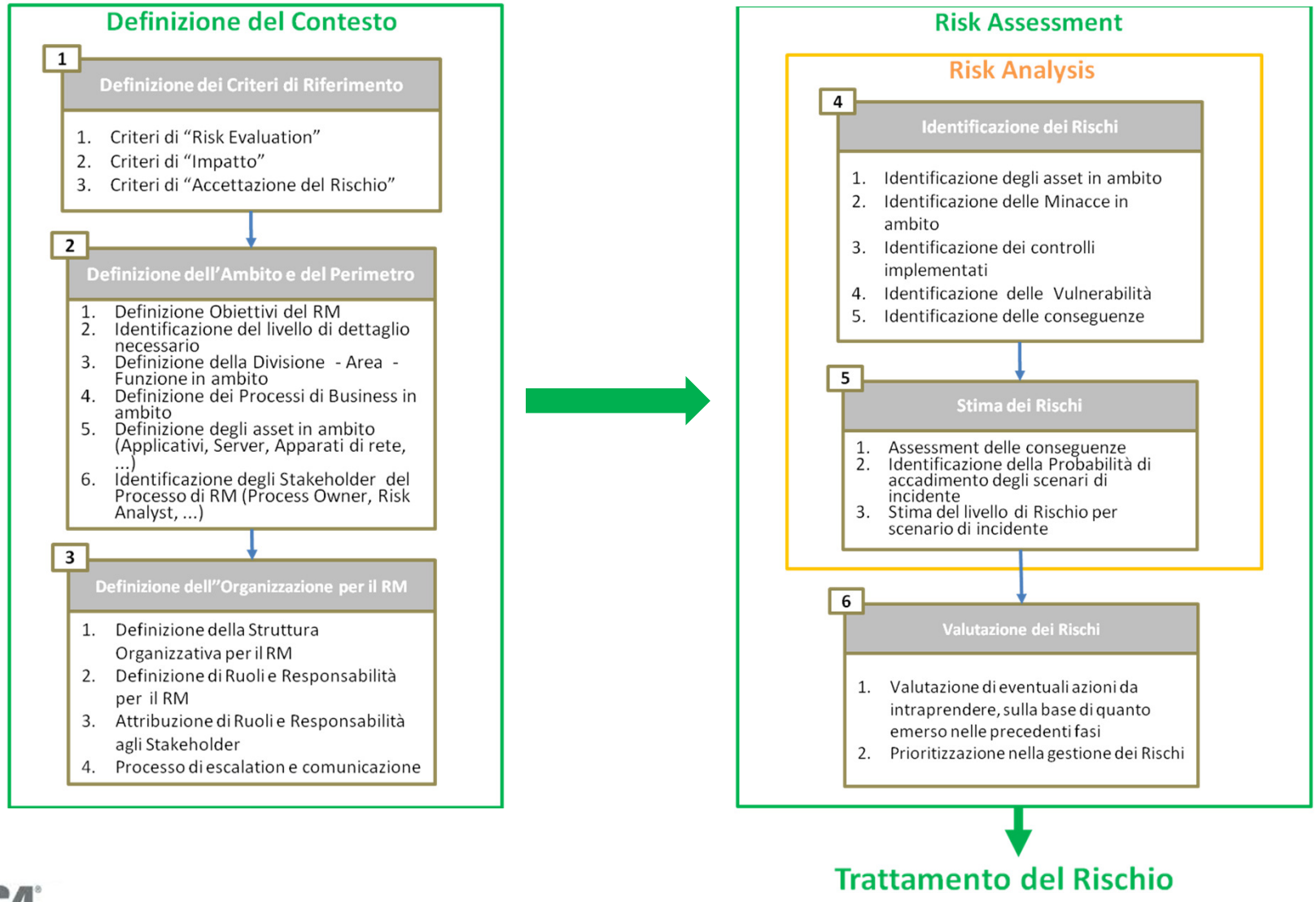
ALE = SLE x ARO

In cui:

SLE = Single Loss Expectancy – stima del danno economico prodotto dall'occorrenza di una minaccia sull'asset in oggetto
ARO = Annualized Rate of Occurence – probabilità che la minaccia in oggetto si manifesti nell'arco temporale di un anno
ALE = Annualized Loss Expectancy – stima del danno economico annuale prodotto dal perpetrarsi di una minaccia nei confronti dell'asset in oggetto

Analisi del contesto – RA (3/4)

Esempio di PROCESSO di IT Risk Assessment(bottom-up)



Analisi del contesto – RA (4/4)

OUTPUT

- *Scenari di disastro*
- *Probabilità accadimento minacce*
- *Livello di esposizione alle minacce*
- *Livelli di vulnerabilità*
- *Livelli di Rischio*

CRITERI DI VALUTAZIONE DELLA MINACCIA				LIVELLO DI ESPOSIZIONEALLA MINACCIA (LEM)
SORGENTE			FREQUENZA	
Capacità	*Intento*	*Valutazione*		
Si	Si	altamente attiva	bassa	MEDIO
			media	ALTO
			alta	
Si	No	mediamente attiva	bassa	BASSO
No	Si		media	MEDIO
			alta	ALTO
No	No	scarsamente attiva	bassa	BASSO
			media	
			alta	MEDIO

PROBABILITÀ DI ATTUAZIONE DELLA MINACCIA (PAM)		LIVELLO DI ESPOSIZIONE ALLA MINACCIA (LEM)		
		Alto	Medio	Basso
LIVELLO DI VULNERABILITÀ (LVmax)	Alto	ALTO	MEDIO-ALTO	MEDIO
	Medio	MEDIO-ALTO	MEDIO	MEDIO-BASSO
	Basso	MEDIO	MEDIO-BASSO	BASSO

Minacce applicabili

Gli scenari di disastro ed i rischi applicabili devono essere valutati rispetto alle minacce applicabili ed ai loro potenziali impatti.

Le minacce possono:

- essere di diversa natura (malfunzionamenti, disastri naturali, sabotaggi, ..)
- comportare impatti su diversa scala (ad es. scala locale, metropolitana, geografica)
- comportare impatti più o meno gravi

Minaccia	Agente di Minaccia	Tipologia	Scala tipica	Potenziale Impatto
Incendio sale DC (tutte)	Cortocircuito maggiore	Malfunzionamento	Sito	ALTO
Allagamento sale DC (tutte)	Esondazione Fiume	Disastri naturali	Sito	ALTO
Distruzione parziale sale DC (tutte)	Terremoto (di grave entità)	Disastri naturali	Sito	MEDIO
Distruzione totale sale DC (tutte)	Terremoto (di entità molto grave)	Disastri naturali	Metropolitana	MOLTO ALTO
Distruzione totale locali Sito Produzione	Terremoto (di entità molto grave)	Disastri naturali	Metropolitana	MOLTO ALTO
Distruzione totale sale DC (tutte)	Attentato	Sabotaggio umano	Sito	ALTO
Inagibilità totale locali Sito Produzione	Esondazione Fiume	Disastri naturali	Sito	MOLTO ALTO
Distruzione/Alterazione dati (sabotaggio)	Manomissione (fattore umano)	Sabotaggio umano	Qualsiasi	MOLTO ALTO
Fuori Servizio prolungato energia elettrica	Fornitori inadempienti	Malfunzionamenti Infrastrutturali	Metropolitana	MOLTO ALTO
Attacco informatico	virus, malware, hacker	Sabotaggio umano	qualsiasi	ALTO
Indisponibilità del personale	Malattie epidemiologiche	Disastri naturali	Metropolitana	ALTO
Inabilità operativa	Gravi disordini polito-sociali	Sabotaggio umano	Qualsiasi	ALTO
Fuori Servizio prolungato connettività TLC	Fornitori inadempienti	Malfunzionamenti Infrastrutturali	Qualsiasi	MOLTO ALTO

Scenari di Disastro

I possibili scenari di disastro considerati sono legati ad eventi disastrosi non pianificati di varia natura che causano:

•Indisponibilità dei sistemi e dei dati

•Indisponibilità delle linee di comunicazione e delle strutture di network

•Inagibilità permanente o temporanea dei locali

•Indisponibilità delle facilities (energia/acqua)

•indisponibilità del personale operativo

A fronte dei diversi scenari di disastro e dei Livelli di Servizio stabiliti, le soluzioni architetturali si articolano tipicamente in:

• Soluzioni a due siti (sito di Produzione – o "Primario" - e sito di "Recovery" o "remoto", o ancora "secondario")

• Soluzioni a tre siti (sito di Produzione, di Recovery e "sito Bunker")

Il sito di Produzione, di Recovery e Bunker possono essere tra di loro:

•"in campus", ovvero ad una distanza dell'ordine del KM

•"in area metropolitana", ovvero ad una distanza massima di poche decine di KM

•"in area geografica", ovvero a distanza "significativa" (oltre i 100 KM circa).

Il sito bunker generalmente non è dotato di risorse elaborative, e quindi è funzionale al solo riallineamento dati del sito remoto in presenza di indisponibilità del sito primario (in questo caso gli applicativi ed i servizi vengono erogati dal sito remoto).

Scenari di Disastro – Soluzione 1

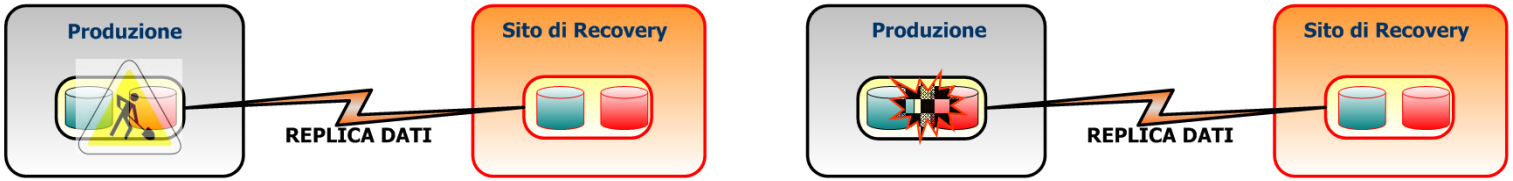
Minacce applicabili:

- Incendio sala DC (locale)
- Allagamento sala DC (locale)
- Manutenzione straordinaria

Livelli di Servizio per i sistemi impattati:

- RTO > 0
- RPO > 0

Soluzione architetturale: soluzione a due siti in area geografica, con replica asincrona dei dati



Scenario di Disastro: indisponibilità parziale del Sito Primario; le capacità elavorative del Sito primario ed i dati sono parzialmente compromessi; nel caso di invocazione dello stato di crisi, la produzione (almeno dei servizi critici) viene erogata dal sito di Recovery.

Scenari di Disastro – Soluzione 2

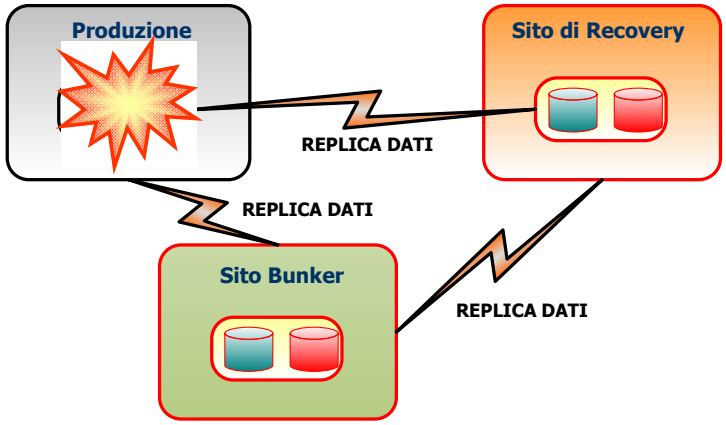
Minacce applicabili:

- Incendio sale DC (tutte)
- Allagamento sale DC (tutte)
- Distruzione parziale sale DC (tutte)
- Distruzione totale sale DC (tutte)
- Distruzione totale
- Inagibilità totale

Livelli di Servizio:

- RTO > 0,
- RPO = 0

Soluzione architetturale: soluzione a tre siti (sito di Produzione e sito Bunker in area metropolitana, sito di Recovery in area geografica rispetto agli stessi), con replica dei dati sincrona (Produzione → Bunker) ed asincrona (Produzione → Recovery, Bunker → Recovery)



Scenario di Disastro: indisponibilità totale del sito Primario; le capacità elavorative ed i dati del Sito primario sono totalmente compromessi; la produzione viene erogata dal sito di Recovery (nel caso in cui il sito bunker presenti dati consistenti più recenti, il sito di recovery si riallinea prima rispetto ai dati del sito bunker).

Scenari di Disastro – Soluzione 3

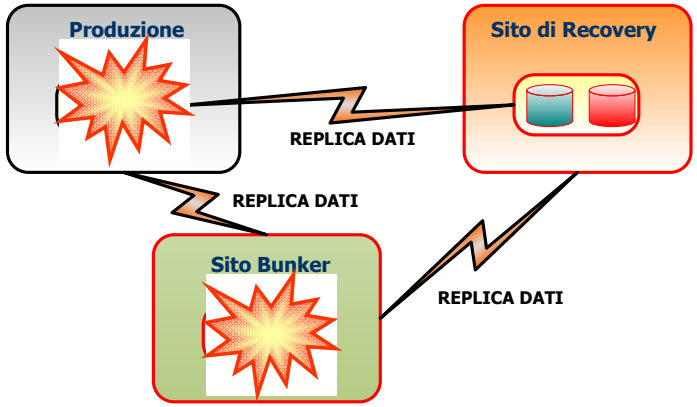
Minacce applicabili:

•Incendio sale DC (tutte)
•Allagamento sale DC (tutte)
•Distruzione totale Sito Primario e (tutte)
•Distruzione totale locali sito Primario

Livelli di Servizio:

- RTO > 0,
- RPO > 0

Soluzione architetturale: soluzione a tre siti (sito di Produzione e sito Bunker in area metropolitana, sito di Recovery in area geografica rispetto agli stessi), con replica dei dati sincrona (Produzione → Bunker) ed asincrona (Produzione → Recovery, Bunker → Recovery)

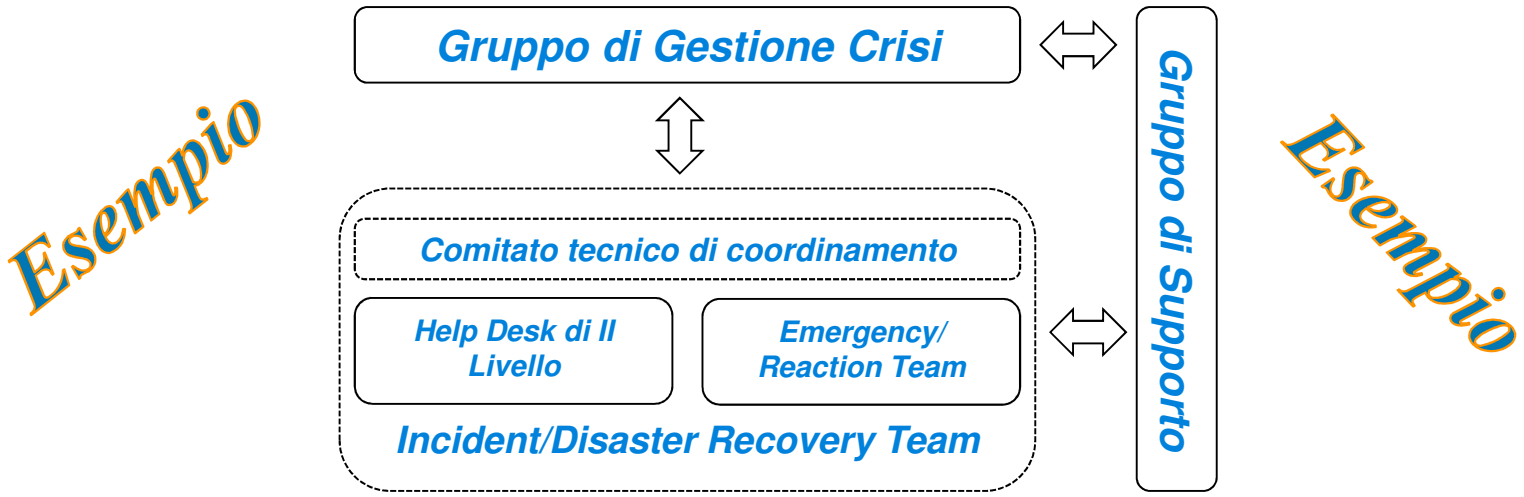


Scenario di Disastro: indisponibilità totale del sito Primario e del sito Bunker; le capacità elavorative ed i dati del Sito primario sono totalmente compromessi; contemporaneamente, è compromesso anche il sito bunker. Il sito secondario, pur non potendo effettuare un eventuale riallineamento con il sito bunker, riprende ad erogare i servizi. Tipicamente questa condizione si ha in seguito all'accadimento di un terremoto di grave entità su vasta scala (agente di minaccia). .

Agenda

- Introduzione alla Business Continuity e al Disaster Recovery
- Analisi del Contesto e degli Scenari di Disastro
- Disaster Recovery – Organizzazione e Documentazione
- La Continuità Operativa per le PP.AA.
- La Continuità Operativa in ambito bancario
- Q&A

Organizzazione ai fini del DR

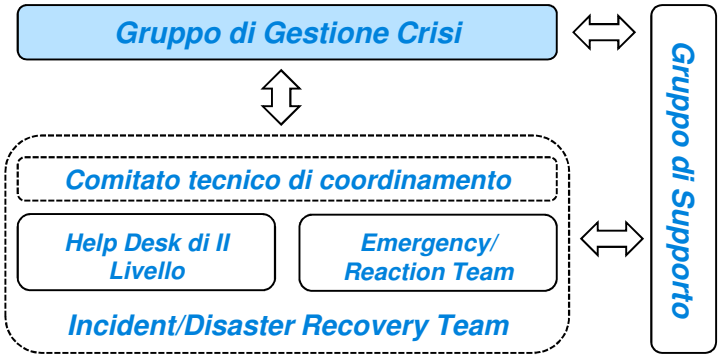


L'organizzazione ai fini del DR viene definita a livello strategico dagli organi direttivi aziendali. Tipicamente, tale organizzazione:

- si inquadra nell'ambito più generale dell'organizzazione ai fini della Continuità Operativa
- si integra con il team di gestione degli incidenti
- Prevede la partecipazione dei ruoli e delle Funzioni chiave aziendali (CxO, Direttori, Funzioni di assurance)
- viene pubblicato all'interno del Piano di Disaster Recovery (DRP)
- è strutturato in diversi gruppi:
    - gruppo di Gestione Crisi
    - incident/Disaster Recovery Team
    - gruppo di Supporto

Organizzazione ai fini del DR - Gruppo Gestione Crisi

Il **Gruppo Gestione 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 ed ha inoltre responsabilità di garanzia e controllo.

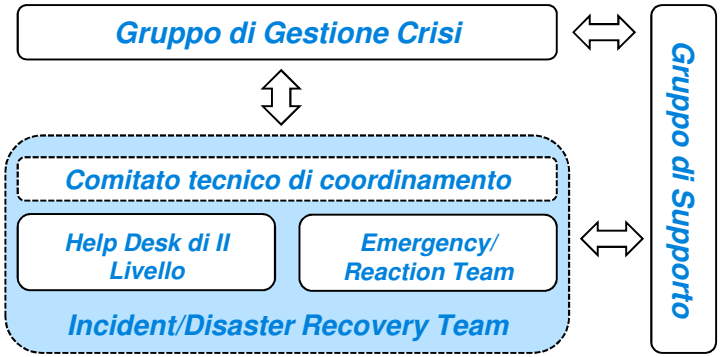


I suoi compiti principali prevedono:

- approvazione del Piano di Disaster Recovery (DRP)
- valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi
- dichiarazione dello stato di "Crisi"
- avvio delle attività di recupero e controllo del loro svolgimento
- attivazione del processo di rientro alle condizioni normali e controllo del loro svolgimento
- gestione dei rapporti interni e risoluzione dei conflitti di competenza
- gestione delle situazioni non contemplate
- convocazione e partecipazione alle riunioni durante lo stato di Crisi
- dichiarazione del ritorno allo stato di "normale operatività" (rientro dallo stato di "Crisi").

Organizzazione ai fini del DR – Comitato tecnico Coordinamento

Il **Comitato tecnico di coordinamento** è il gruppo tecnico che gestisce e coordina le attività del team di Help Desk di II Livello e di Emergency/Reaction.



I suoi compiti principali sono:

• definizione dell'istante di partenza dell'RTO

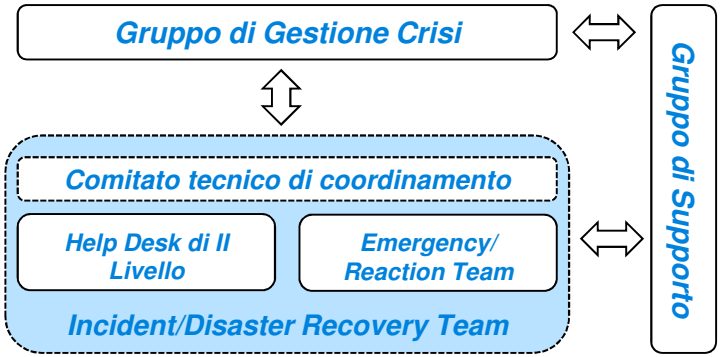
• aggiornamento costante del Gruppo Gestione Crisi sull'evoluzione degli incidenti con severità pari ad Alta o Crisi

• Interfaccia con gli i fornitori/service provider in condizioni di crisi

• coordinamento del personale operativo in emergenza

• gestione del budget per spese straordinarie legate all'emergenza

Organizzazione ai fini del DR – HD II Livello



Il **team di Help Desk di II Livello** ha come compito principale quello di eseguire attività di analisi degli incidenti di sicurezza, ed in particolare:

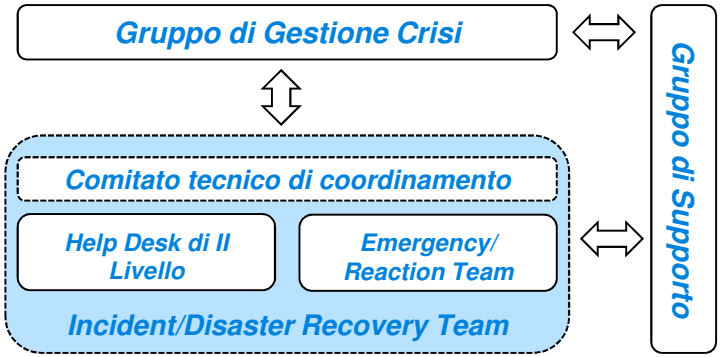
- rafforzamento del normale help desk di primo livello in caso di emergenza
- analisi approfondita degli incidenti al fine di valutare la severità dell'emergenza, secondo le modalità riportate nel piano di DR
- Attivazione del Gruppo Gestione Crisi, attraverso il Comitato tecnico di coordinamento, qualora la severità dell'incidente prefiguri lo status di "Crisi"
- organizzazione dei trasporti e della logistica del personale operativo in emergenza
- attivazione dell'Emergency Team qualora la severità dell'incidente sia pari ad "Alta"
- aggiornamento dei sistemi di gestione della conoscenza a supporto degli operatori del normale help desk (riguardo alle tematiche da affrontare in caso di emergenza),
- esercitazioni e simulazioni periodiche

Il gruppo è composto da presidi afferenti a diverse strutture di intervento tecnico (anche appartenenti a fornitori/service provider) quali:

- Gruppi Operation TLC
- Gruppi Control Room (CR)
- Gruppi Data Center (DC)
- Gruppi di Service Manager (SM

Organizzazione ai fini del DR – Emergency/Reaction Team

Lo **Emergency/Reaction Team** ha il compito di effettuare, a valle della dichiarazione dello stato di "Crisi", tutte le attività necessarie a proteggere gli asset aziendali ed a ripristinare la normale operatività.



A tal fine, il Team ha i seguenti compiti:

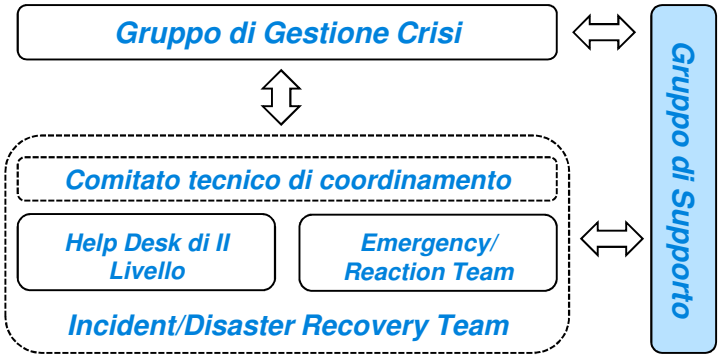
- manutenzione dell'infrastruttura tecnologica e applicativa di recupero
- responsabilità di tutte le attività sulle applicazioni e i dati ad esse associati
- responsabilità di tutte le operazioni che coinvolgono i sistemi informatici e la rete di Telecomunicazioni,
- attuazione delle istruzioni operative di ripristino del servizio in condizioni di disastro
- attuazione delle istruzioni operative di ripristino del servizio in condizioni di simulazione di disastro
- monitoraggio del funzionamento delle applicazioni e dei sistemi in configurazione di ripristino
- esercitazioni e simulazioni periodiche

Il gruppo è composto da presidi afferenti a diverse strutture di intervento tecnico (anche appartenenti a fornitori/service provider) quali:

- Gruppi Operation TLC
- Gruppi Control Room (CR)
- Gruppi Data Center (DC)
- Gruppi di Service Manager (SM)

Organizzazione ai fini del DR - Gruppo di Supporto

Il **Gruppo di Supporto** è una struttura amministrativa che fornisce supporto al Gruppo Gestione Crisi.



I suoi compiti principali prevedono:

- Supporto nella redazione e nell'aggiornamento periodico del DRP (compreso l'aggiornamento dei riferimenti interni del personale)
- L'adeguamento periodico dell'analisi di impatto (Business Impact Analysis)
- lo studio di scenari di emergenza e definizione delle strategie di rientro
- l'attuazione delle attività di divulgazione e di sensibilizzazione interna sui temi della continuità
- la convocazione e la partecipazione alle riunioni ordinarie e straordinarie
- la verbalizzazione delle riunioni ordinarie e straordinarie

Documentazione a supporto del DR

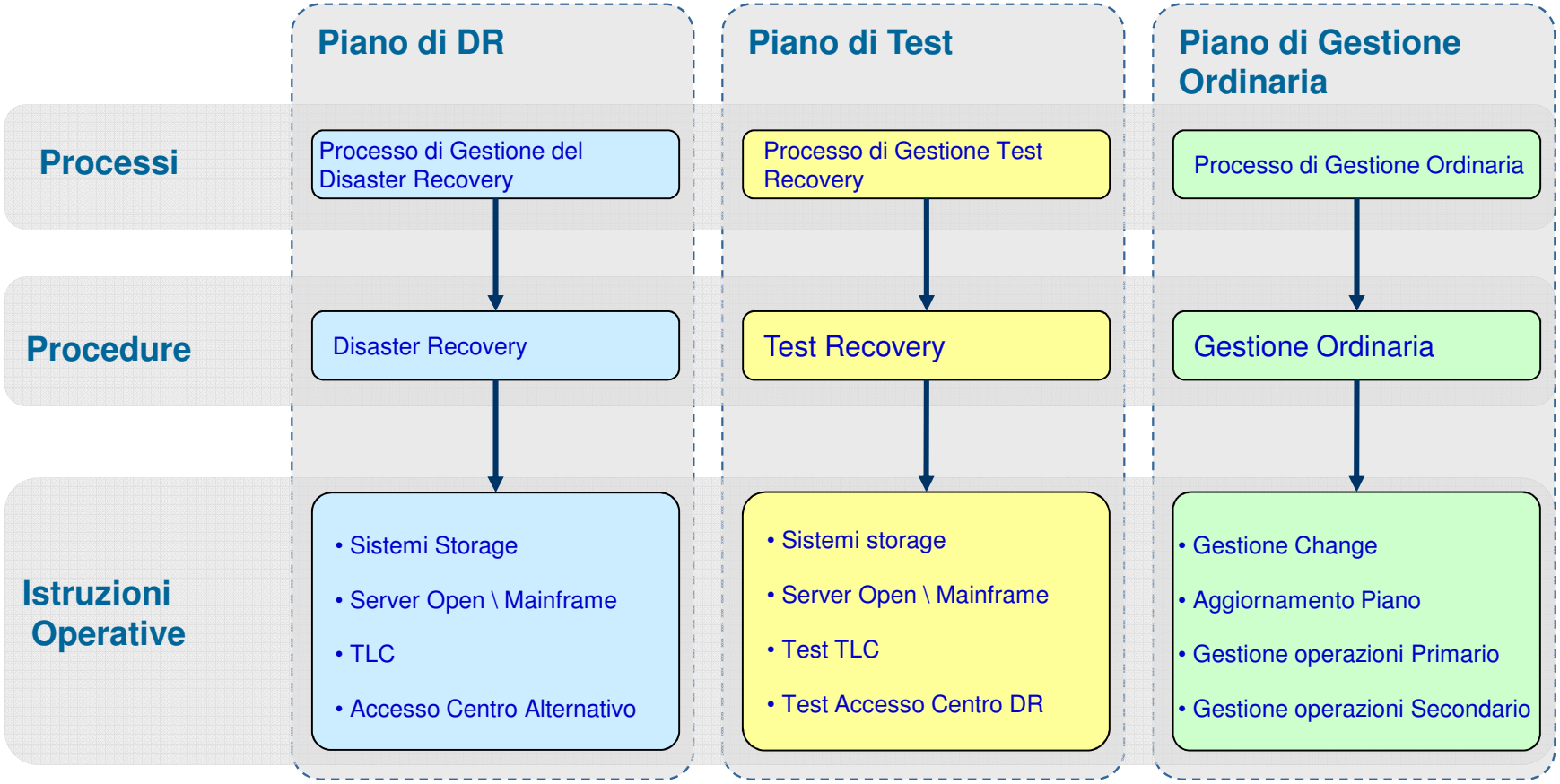
- **Documentazione** per la **Gestione** della soluzione di Disaster Recovery

  Cosa occorre **Gestire**:

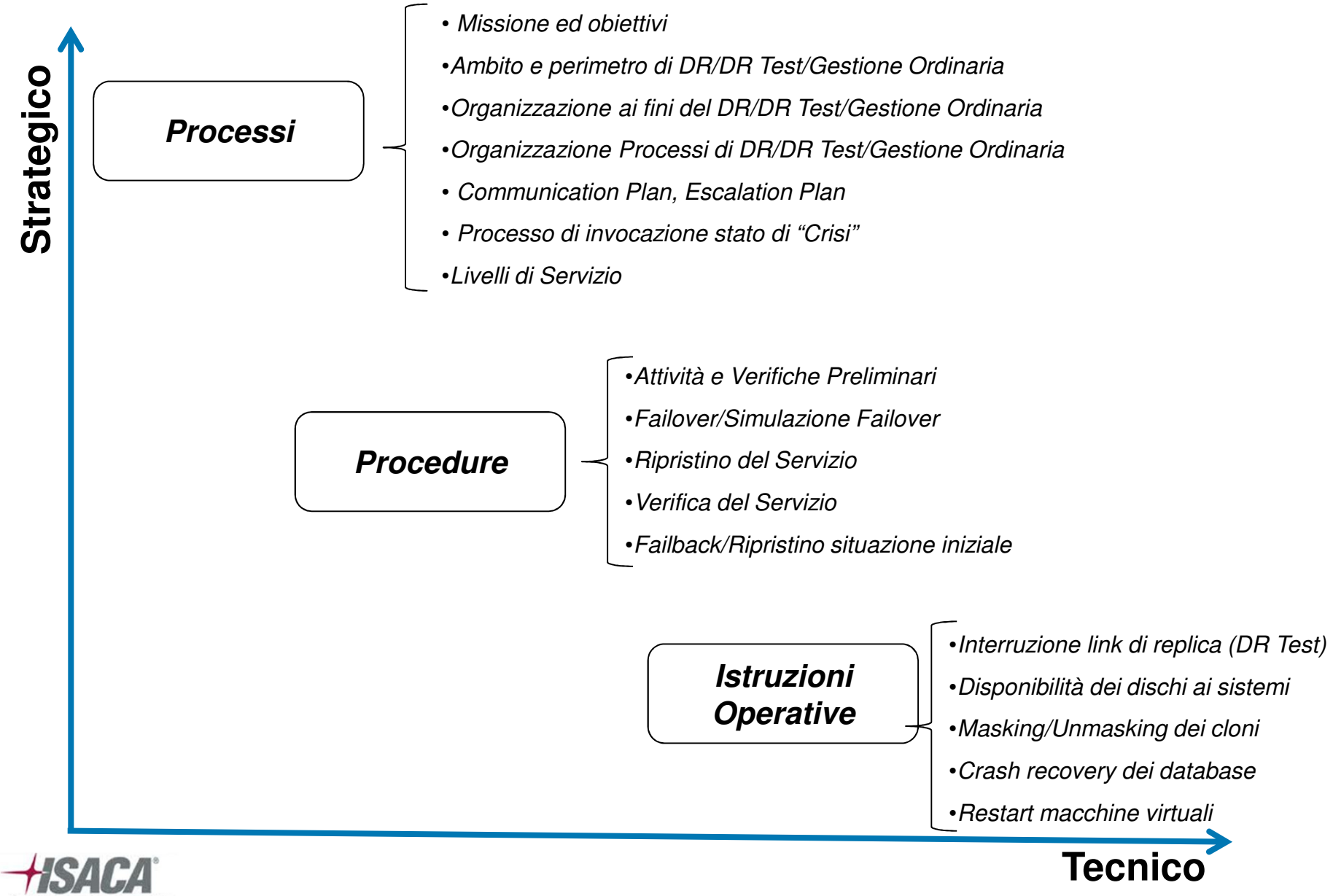
  – Tecnologia addizionale per il DR
  – Procedure per la garanzia della consistenza (dato / app)
  – Correlazioni-dipendenze ambienti DR-Produzione (processi, procedure)
    - Patching app/OS
    - Changes
    - Provisioning
  – Test periodici (prescrizioni BI)
  – Eventuali failures (es. links, dischi)
  – etc…

Documentazione a supporto del DR - Framework

- Piano di DR, per la gestione della situazione di reale emergenza;
- Piano di Test, per la simulazione periodica del recovery e verifica dell'efficacia della soluzione;
- Piano di Gestione Ordinaria, per la quotidiana manutenzione e controllo della soluzione.



Documentazione a supporto del DR - Contenuti



Documentazione a supporto del DR – Definizioni

- **Piano di DR**:

  insieme di documenti che definiscono la gestione di una situazione di reale o presunta emergenza a partire dalla generazione e trasmissione dell'allarme fino al ripristino dell'infrastruttura completa sui siti di Disaster Recovery.

- **Piano di Test del DR**

  insieme di documenti che definiscono come portare a termine periodiche simulazioni di recovery dei sistemi a seguito di disastro, al fine di verificare l'efficacia della soluzione di DR, a seguito delle operazioni previste nella gestione ordinaria.

  Da non confondere con il collaudo dell'infrastruttura.

- **Piano di Gestione Ordinaria**

  insieme di documenti che definiscono il *modus operandi* nella quotidiana manutenzione e controllo dei sistemi che fanno parte della soluzione di DR.

  Da non confondere con i processi di gestione dell'infrastruttura di produzione.

Sui tre ambiti la documentazione si struttura in
Processi, Procedure e Istruzioni operative.

Documentazione a supporto del DR – Processi (1/2)

Cos'è un processo

Il processo (aziendale) *o business process* è un insieme di attività correlate, svolte all'interno dell'azienda, che prendono in ingresso risorse (*input del processo*) producendo un prodotto (*output del processo*) destinato ad un soggetto interno o esterno all'azienda (*cliente*).

La trasformazione dell'input in output può essere eseguita con l'impiego di lavoro umano, di macchine o di entrambi.

Il processo è teso al raggiungimento di un obiettivo aziendale.

In un processo sono normalmente coinvolti più organi aziendali *(attori)* e il loro apporto è coordinato attraverso un flusso di informazioni (*workflow*).

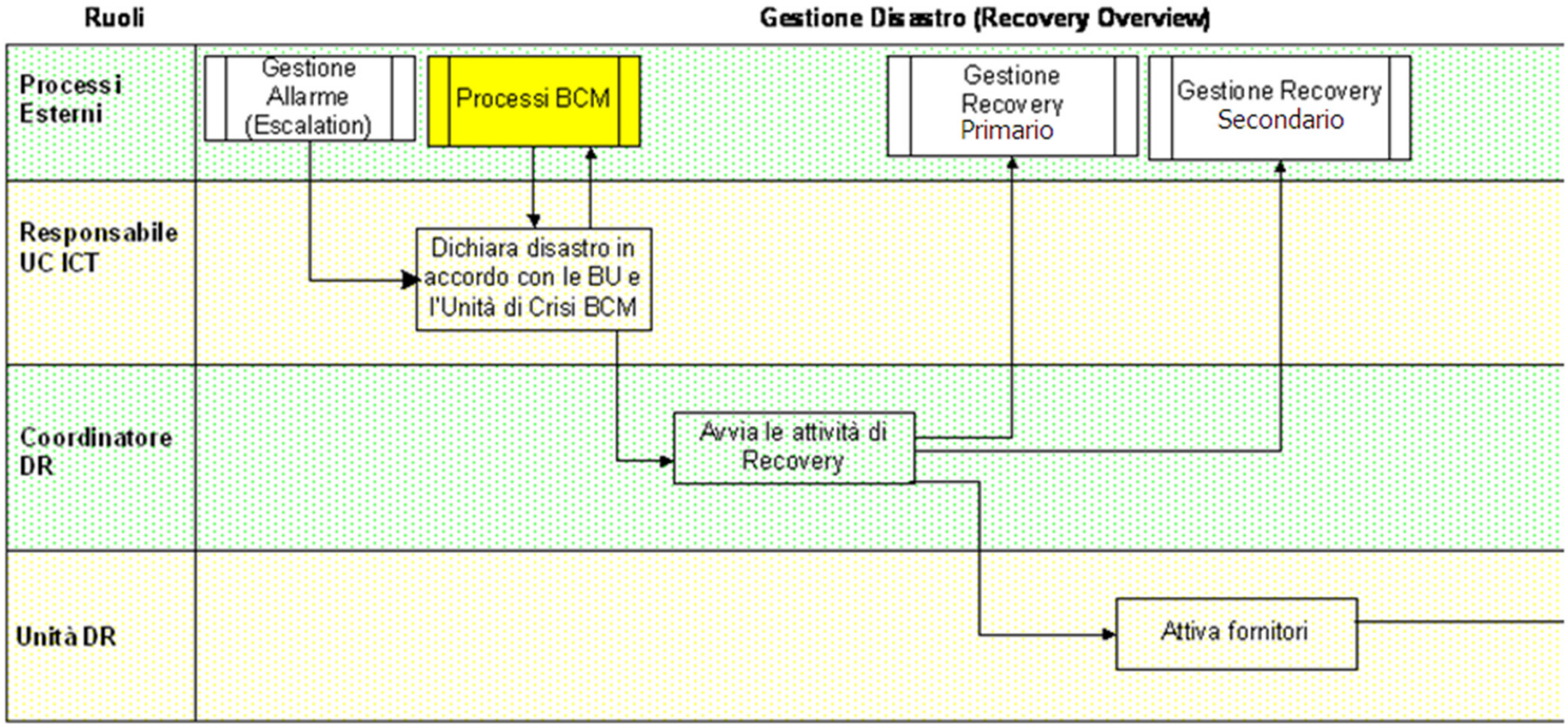
Un sotto-processo è una parte del processo che comprende più attività e ha propri attributi in termini di obiettivo, input e output, contribuendo però nel contempo al raggiungimento dell'obiettivo più generale del processo:

Obiettivo dei Processi di gestione del DR è la gestione del Disastro e il mantenimento in efficienza della soluzione di DR mediante test periodici ed esercizio ordinario.

Documentazione a supporto del DR – Processi (2/2)

Esempio di documento di Processo

- *Un esempio di flusso presente nei documenti di Processo.*



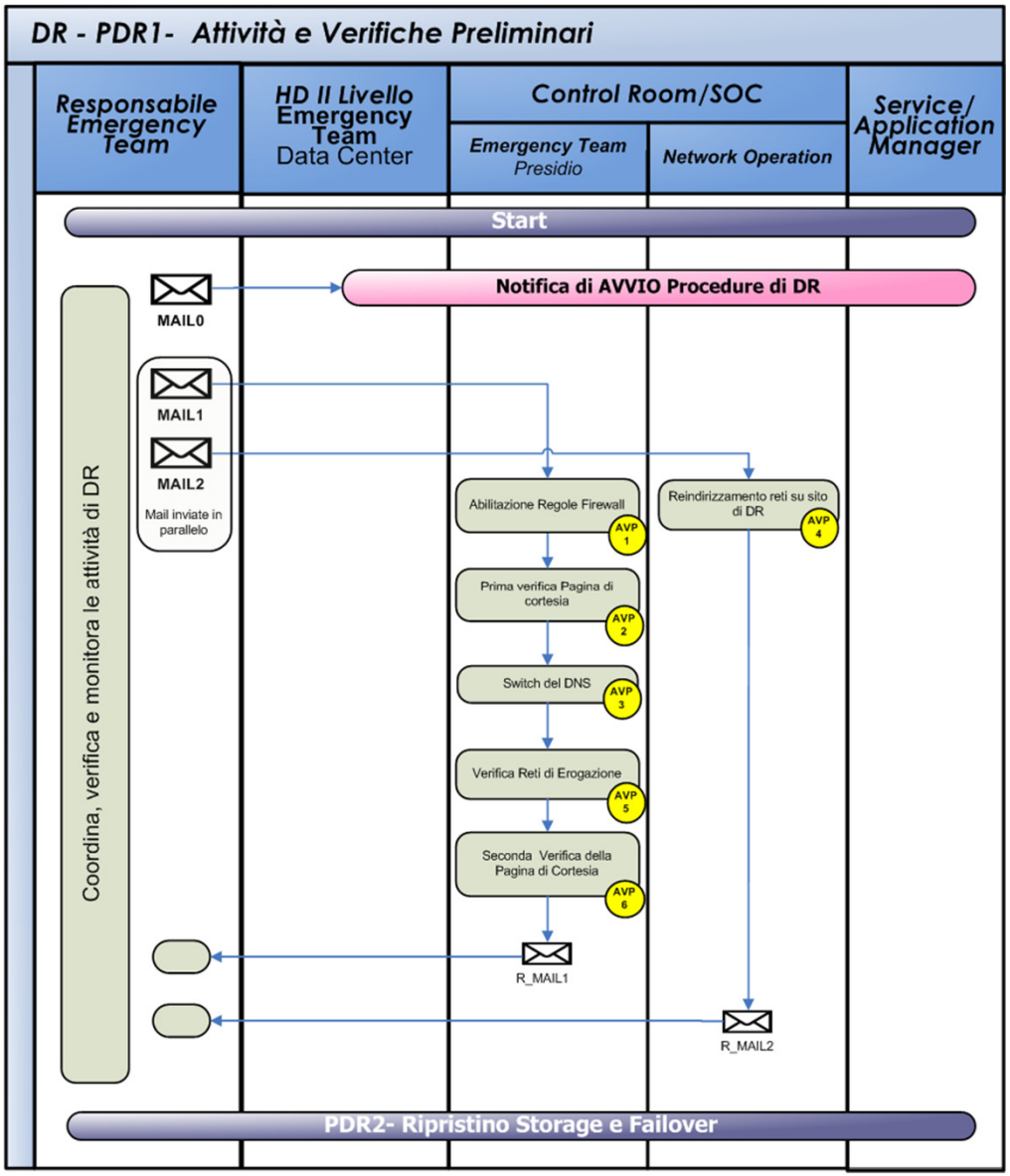
Documentazione a supporto del DR – Flusso di Comunicazione

Al fine di agevolare le operazioni dei diversi gruppi operativi, spesso sono utili dei "Flussi di comunicazione" dettagliati per ogni Procedura Operativa, riportante:

-Tutti i principali referenti e gruppi operativi coinvolti nella Procedura

-Tutte le istruzioni operative, nella corretta sequenza

- Le notifiche di ingaggio tra i diversi referenti/gruppi (ad esempio tramite email)



Documentazione a supporto del DR – Procedure (1/2)

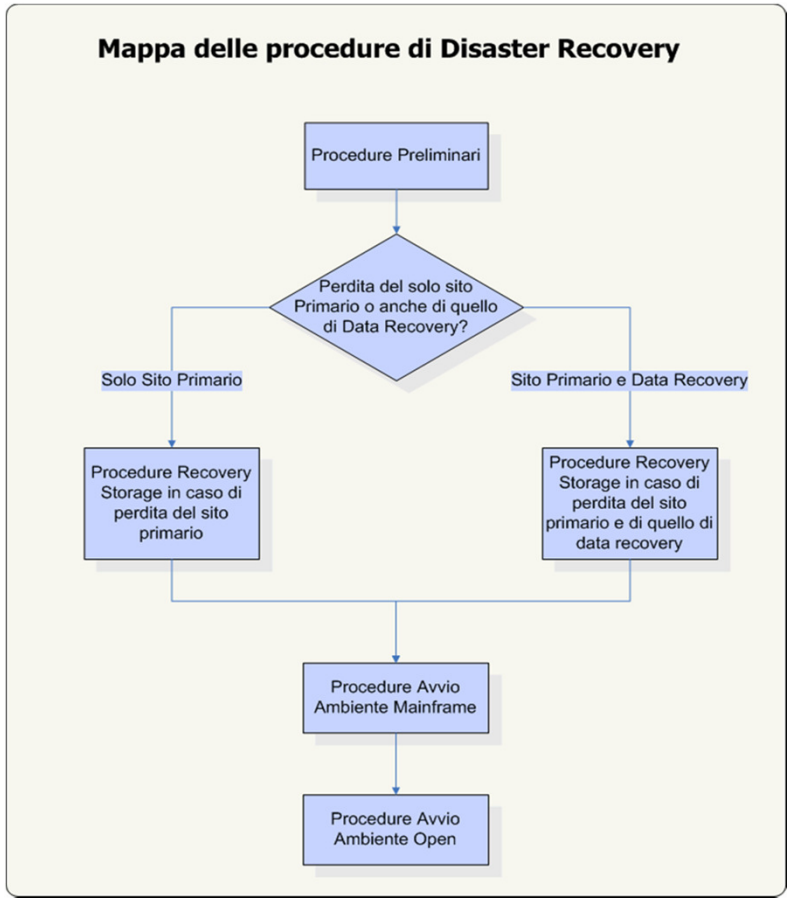
Cos'è una procedura

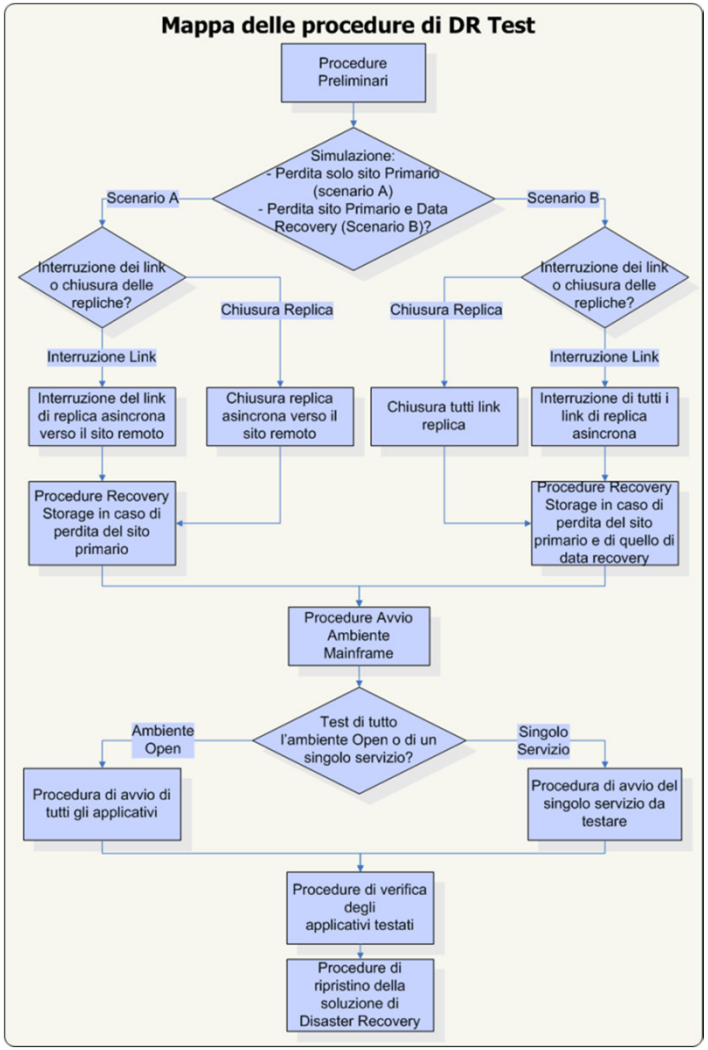
Una procedura è una parte di un processo o sotto-processo che **non include decisioni** e che quindi può non essere scomposta ulteriormente (sebbene la scomposizione sia di per sé possibile).
Le procedure possono essere portate a termine con operazioni su oggetti fisici o informatici oppure con una **scelta** assunta da un *attore* coinvolto nel processo.

Obiettivo delle procedure di gestione della soluzione di DR è quello di supportare i sotto-processi di gestione del DR nel mantenere in efficienza la soluzione di DR mediante test periodici ed esercizio ordinario, e nella gestione del Disastro.

Documentazione a supporto del DR – Procedure (2/2)

Esempio di documento di Procedure



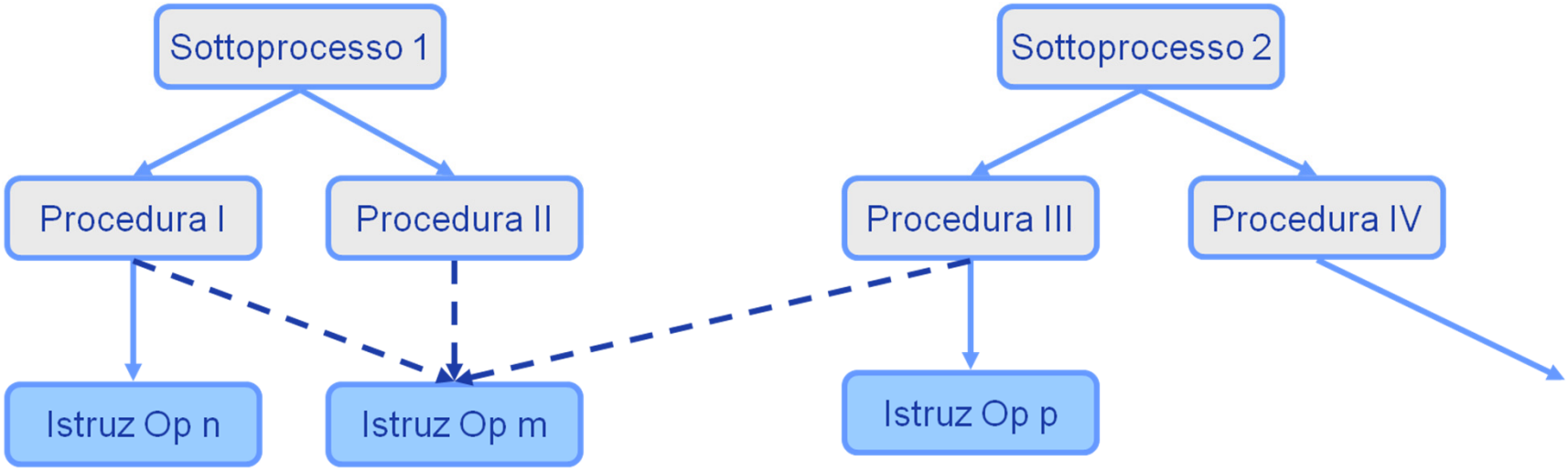


Documentazione a supporto del DR – Istruzioni Operative (1/2)

Cos'è un'istruzione operativa

Un'istruzione operativa è una sequenza di passi determinati che concorrono alla conclusione positiva della procedura.

Un'istruzione operativa può essere richiamata da più di una procedura.



Documentazione a supporto del DR – Istruzioni Operative (2/2)

Esempio di documento di Istruzione Operativa

SAN: VERIFICA DELLO STATO DEI VOLUMI R1 E R2	**ID: AVPN**
SCOPO: Verifica dello stato dei dischi R1, R2 e delle coppie di volumi e delle coppie R2 CLONI sul sito remoto ed eventuale risicnronizzazione dei CLONI	
MODALITÀ DI ESECUZIONE: Accedere alla... Il comando che verifica lo stato dei volumi può essere lanciato su entrambi i box storage ed è il seguente: symrdf -cg xxxxx query Il comando restituisce lo stato dei dischi R1 e R2 e lo stato delle coppie di volumi. symclone -cg xxxxx query Il comando restituisce lo stato dei dischi R2 CLONI. In questo scenario i volumi R1 sono RW (“Read&Write”), gli R2 in WD (”Write Disable”) e lo stato delle coppie di volumi è “Synchronized”, e lo stato dei CLONI è “Copied” (“Read&Write”) come visualizzato in Figura. **<SCREENSHOT>** Effettuare una risincronizzazione dei CLONI e verificarne successivamente lo stato (per lavorare su dati più aggiornati), eseguendo i comandi: symclone –cg xxxx recreate –tgt –precopy symclone –cg xxxx query Qualora non si riuscisse a completare le istruzioni sopra indicate, contattare immediatamente il responsabile del Team di Incident/Disaster Recovery	
RISULTATO ATTESO: Volumi R1 in modalità RW (“Read&Write”); volumi R2 in modalità WD (”Write Disable”); stato delle coppie di volumi : Synchronized; stato dei CLONI R2: Write Disabled	

Agenda

- Introduzione alla Business Continuity e al Disaster Recovery
- Analisi del Contesto e degli Scenari di Disastro
- Disaster Recovery – Organizzazione e Documentazione
- La Continuità Operativa per le PP.AA.
- La Continuità Operativa in ambito bancario
- Q&A

Adempimenti art. 50-bis nuovo CAD

DigitPA

DigitPA (ex CNIPA - Centro nazionale per l'informatica nella pubblica amministrazione), è l'ente pubblico per l'attuazione delle politiche del ministro per l'innovazione e le tecnologie.

ADEMPIMENTI

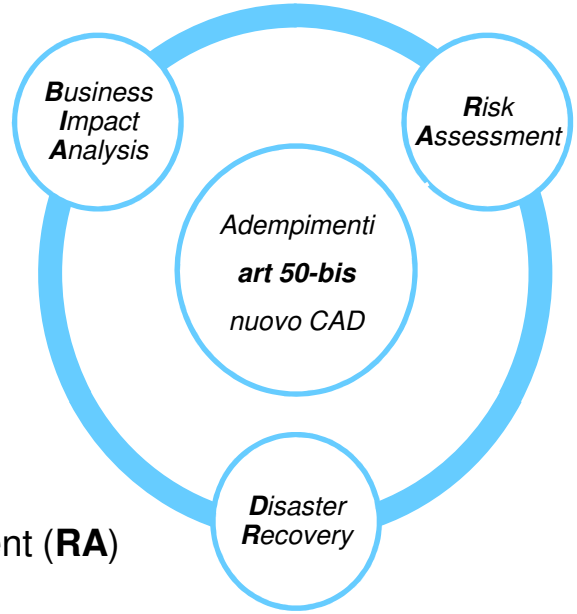
Adempimenti previsti dall'articolo **50-bis** (Continuità Operativa) del CAD:

- Autovalutazione
- Studio di Fattibilità Tecnica (SFT)
- Piani di Continuità Operativa (CO)/Disaster Recovery (DR)

Adempimenti art. 50-bis nuovo CAD

ANALISI DEL CONTESTO – PERCHE'

"La redazione dello Studio di Fattibilità Tecnica è il momento finale di un percorso metodologico che l'Amministrazione deve effettuare"...
"senza voler prescindere dai percorsi e dalle metodologie esistenti, con particolare riguardo alla BIA e alla RA".



LE METODOLOGIE A SUPPORTO

- Analisi di Contesto: Business Impact Analysis (**BIA**) e Risk Assessment (**RA**)
- Metodologie a supporto del **DR**

Quadro normativo

*"Assicurare a qualsiasi livello (Stato, Regioni, autonomie locali) la **disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità** dell'**informazione** in **modalità digitale**" (articolo 2)*

*"le **strategie** sono quelle della riorganizzazione ed aggiornamento dei servizi resi dalle **pubbliche amministrazioni** sviluppando a tal fine l'**uso delle tecnologie dell'informazione e della comunicazione**..." (articolo 7).*

***Codice di Amministrazione Digitale** (CAD)*
D.Lgs 7 marzo 2005, n. 82

Introduzione dell'art. 50 bis - "Continuità Operativa" (CO).

Obbligo per le PP.AA. di redigere:
***a) un piano di continuità operativa**, che fissa gli obiettivi e i principi da perseguire nella pratica della gestione della continuità operativa, descrivendo anche le preposte procedure.;*
***b) il piano di disaster recovery (DR)** come parte integrante del piano di continuità operativa.*

DigitPA detta gli standard di riferimento, funge da organo revisore, e relaziona al DPAS

***Nuovo CAD -** modifiche ed integrazioni del D.Lgs 30 dicembre 2010, n. 235*

Illustra le attività di competenza di DigitPA e delle Amministrazioni in merito all'attuazione dell'art. 50 bis.

*La **prima parte** riporta le informazioni che le PP.AA. devono inviare a DigitPA ai fini del rilascio del parere sugli Studi di Fattibilita' Tecnica (SFT) e le modalità di presentazione delle richieste.*
*La **seconda parte** riporta le informazioni che le PP.AA. devono inviare a DigitPA ai fini dell'attivita' di verifica del costante aggiornamento dei Piani di DR*

***CIRCOLARE** 1° dicembre 2011 , n. 58*
Attività di DigitPA e delle Amministrazioni ai fini dell'attuazione degli adempimenti previsti dall'articolo 50-bis del CAD

Contesto

TRANSITORIO

Chi

- Tutte le PP.AA.

Cosa

- In ottemperanza all'art 50-bis del nuovo CAD - D.Lgs. N. 82/2005:
  - Eseguire apposita autovalutazione
  - Redigere lo Studio di Fattibilità Tecnica (SFT)
  - Implementare le soluzioni dettagliate nello SFT
  - Definire i Piani di CO/DR
  - Sottoporre quanto prodotto al parere di DigitPA

Quando

- Entro il 25 aprile 2012 (15 mesi dall'entrata in vigore del D.Lgs.)

A REGIME

Chi

- Tutte le PP.AA.

Cosa

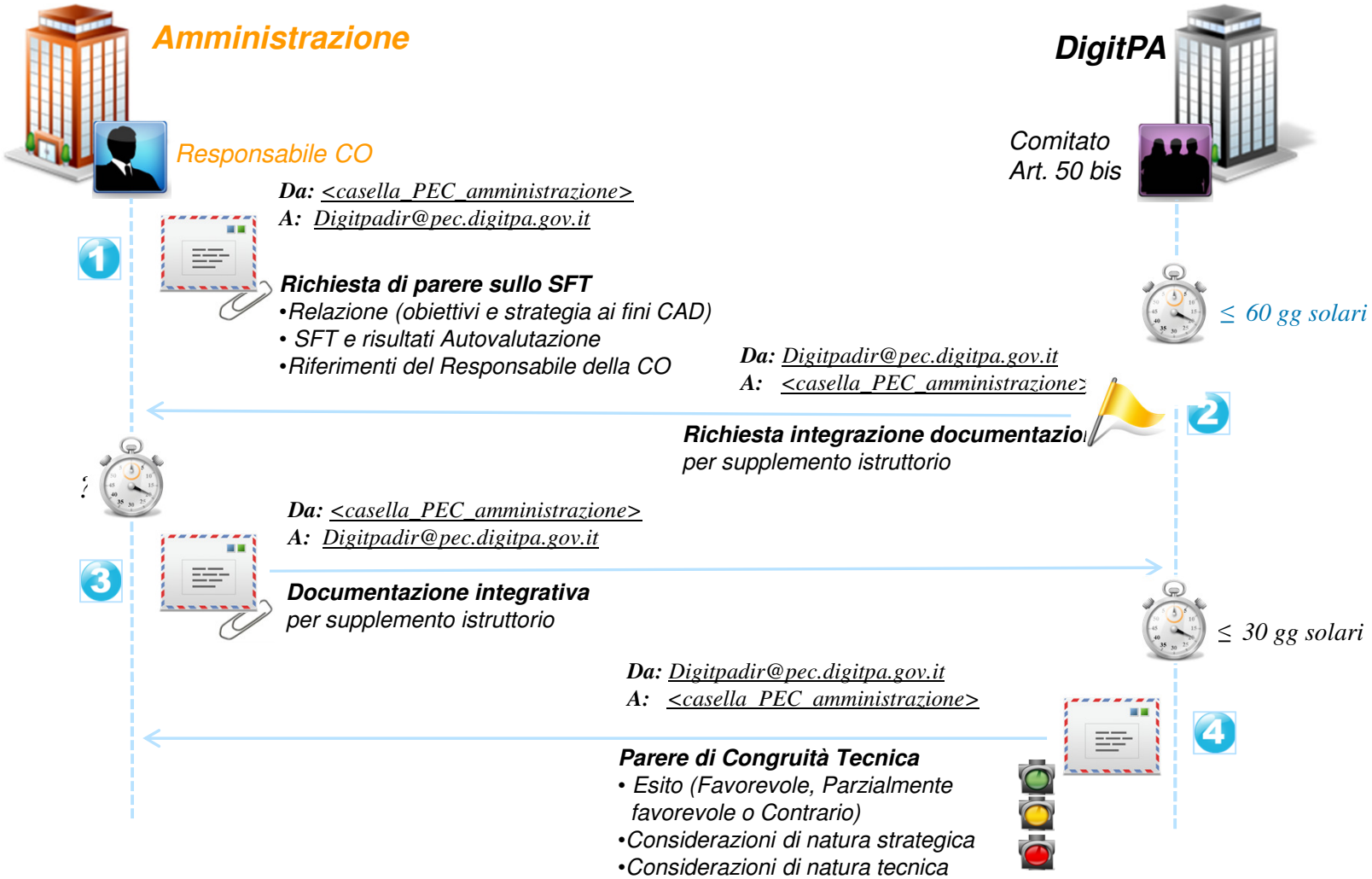
- In ottemperanza all'art 50-bis del nuovo CAD - D.Lgs. N. 82/2005:
  - Implementare le modifiche evolutive delle soluzioni
  - Mantenere aggiornato il Piano di CO
  - Mantenere aggiornato il Piano di DR

Quando

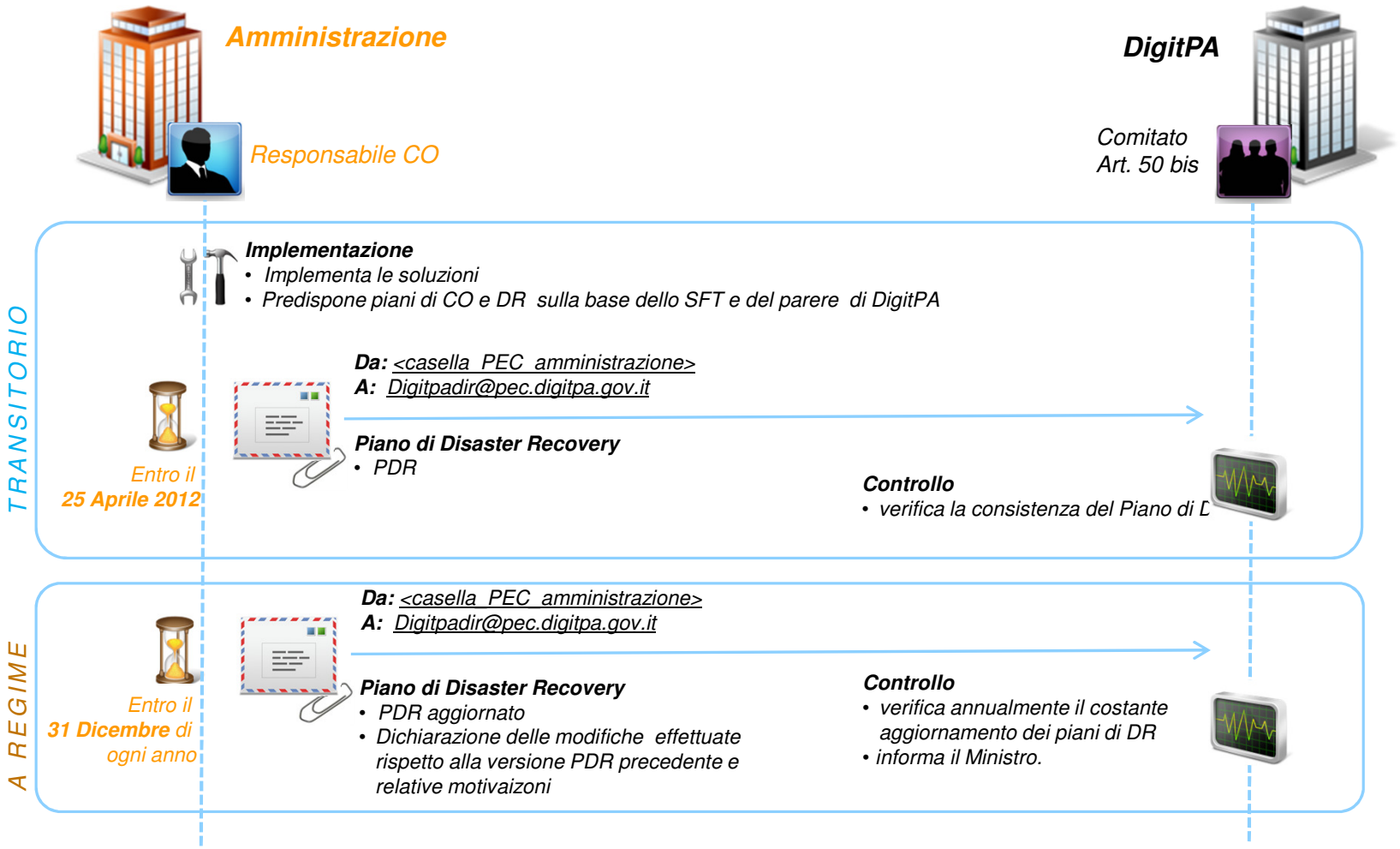
- PP.AA:
  - Invio a DigitPA del Piano di DR specificando le modifiche apportate rispetto all'ultima versione - entro il 31 dicembre di ogni anno
  - Verifica biennale della funzionalità del Piano di CO
- Verifica da parte di DigitPA:
  - annuale: aggiornamento del Piano di DR

Il Processo – SFT (caso 1)

Il Processo – SFT (caso 2)



Il Processo – PDR



Le linee guida (LG)

DigitPA, sentito il Garante della protezione dei dati personali, ha approvato il **16 novembre 2011** le: "*Linee guida per il disaster recovery delle Pubbliche Amministrazioni, ai sensi del comma 3, lettera b) dell'art. 50-bis del DLgs. N. 82/2005 e s.m.i.*"

*"Il percorso di autovalutazione e lo schema di Studio di Fattibilità Tecnica [...] dovranno essere adottati da tutte le Amministrazioni sia che abbiano già adottato soluzioni e piani di CO/DR – come strumento per sottoporre al parere di DigitPA la soluzione in essere e verificarne l'**aderenza alle linee guida** – sia che debbano adottare ex novo lo studio di fattibilità tecnica e sulla base dello stesso i piani di CO/DR".*

OBIETTIVO

Fornire gli strumenti utili per ottemperare agli obblighi introdotti dall'art. 50-bis del CAD

http://www.digitpa.gov.it/fruibilita-del-dato/continuita-operativa

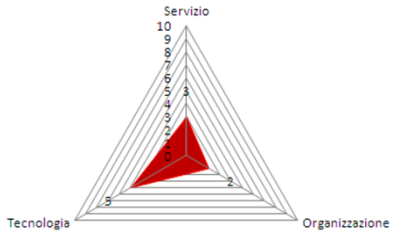
Linee guida – Autovalutazione (1/3)

Consente di identificare i requisiti che l'Amministrazione deve soddisfare in termini di CO/DR sulla base delle caratteristiche peculiari dell'Amministrazione stessa.

Ogni Amminstrazione viene caratterizzata secondo tre direttrici.

DIRETTRICI

- ***Tipologia di servizio erogato*** *- tipologia, numerosità e criticità dei servizi erogati, in termini di danno per l'organizzazione e/o per i suoi utenti in caso di mancata erogazione del servizio stesso*
- ***Complessità organizzativa*** *- aspetti legati alla complessità amministrativa e strutturale dell'organizzazione, al fine di stimare il dimensionamento delle soluzioni tecniche da adottare*
- ***Complessità tecnologica*** *- fattore tecnologico in termini di dimensione e complessità, al fine di poter stimare la tipologia e la natura delle soluzioni tecniche da adottare*

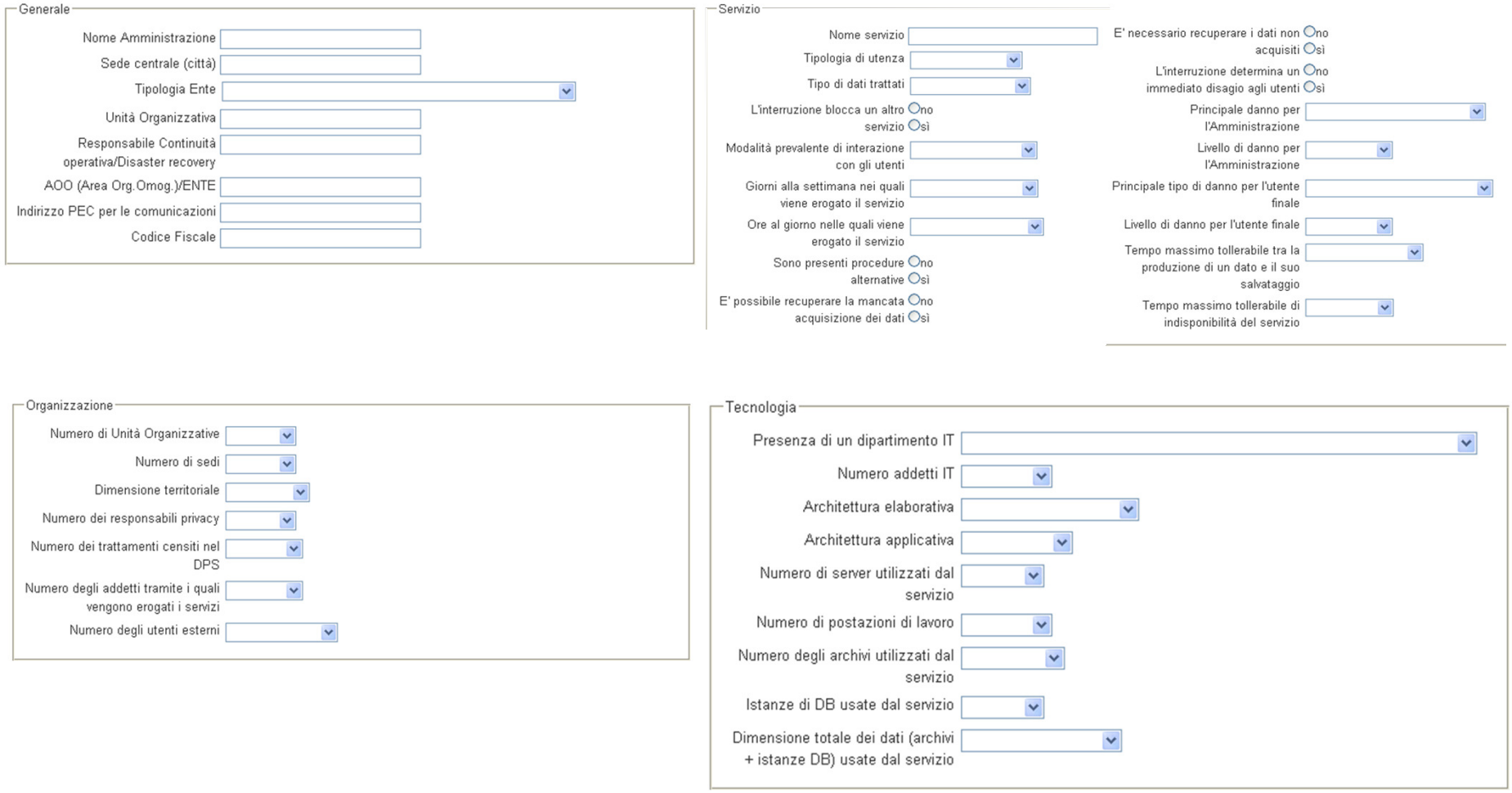


SEZIONI

1. ***Generale*** *- descrizione generale dell'Amministrazione;*
2. ***Servizio*** *- valutazione della direttrice del servizio;*
3. ***Organizzazione*** *- valutazione della direttrice dell'organizzazione;*
4. ***Tecnologia*** *- relativa alla valutazione della direttrice della tecnologia.*

E' possibile effettuare l'autovalutazione utilizzando il form messo a disposizione da DigitPA al seguente indirizzo:
http://apps.digitpa.gov.it/Autovalutazione/web/autovalutazione.php

Linee guida – Autovalutazione (2/3)



Linee guida – Autovalutazione (3/3)

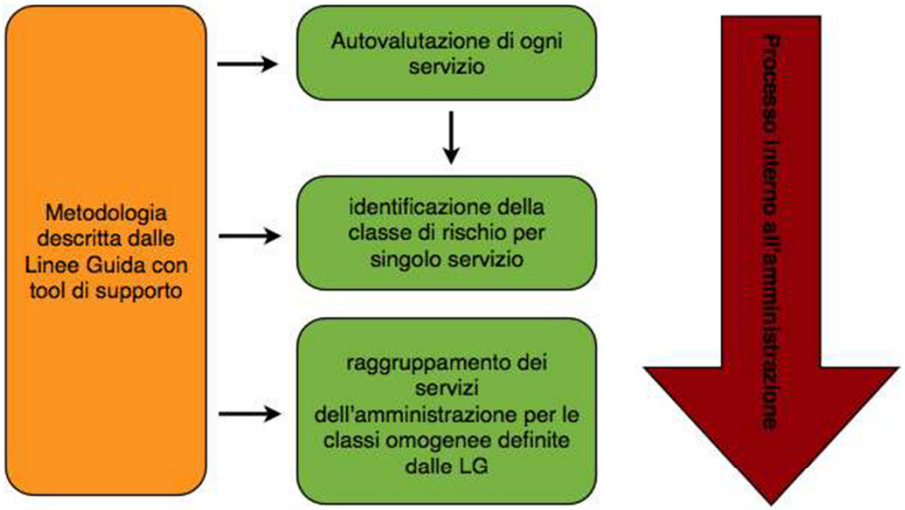
*Tramite gli indicatori per ogni direttrice si ottiene un **indicatore complessivo di criticità**.*

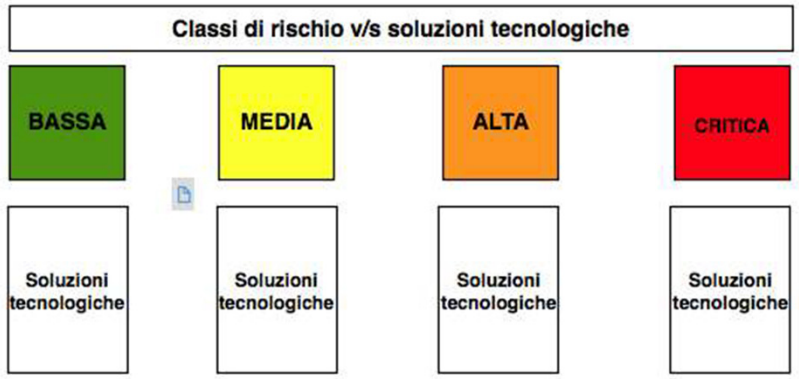
*Le **4 classi** di rischio dei livelli di criticità sono:*

CLASSI DI RISCHIO

- *Bassa*
- *Media*
- *Alta*
- *Critica*

*Per ogni classe di rischio viene associata una soluzione tecnologica (**tier**) minima.*





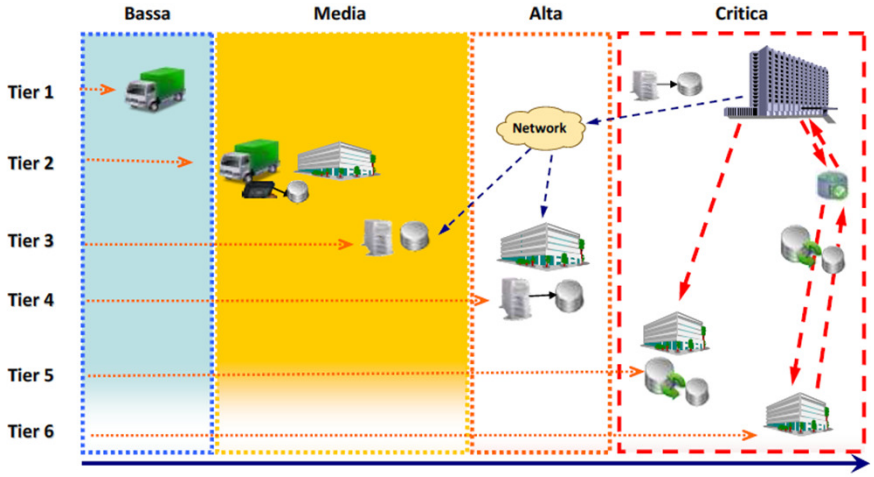
Linee guida - Soluzioni tecnologiche (Tier)

STRUTTURA

***Tier 1**: backup dati e conservazione presso un altro sito con spazi attrezzati per accogliere risorse elaborative in caso di disastro, con garanzia della disponibilità di risorsa di elaborazione in emergenza.*

***Tier 2**: soluzione simile a quella di Tier 1 ma le risorse elaborative, già presenti, possono essere disponibili in tempi più brevi.*

***Tier 3**: soluzione simile a quella di Tier 2 ma il trasferimento dei dati tra il sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti.*



***Tier 4**: la soluzione prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi.*

***Tier 5**: la soluzione è analoga a quella del Tier4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti.*

***Tier 6**: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente speculari a quelle del sito primario, rendendo così possibile ripristinare l'operatività dell'IT in tempi molto rapidi.*

SFT – Introduzione

STRUTTURA

1 - Introduzione

2 - Informazioni generali

3 - L'ambito dello studio di fattibilità tecnica

4 - Il risultato del percorso di autovalutazione

5 - La/e soluzione/i tecnologica/e tecnica/che

6 - Tempi e modalità di realizzazione della soluzione

ALLEGATI

TIPOLOGIA SERVIZI IN AMBITO

DigitPA consiglia di "utilizzare il criterio dei servizi "esposti al pubblico", cioè quelli che offrono le proprie funzionalità a utenti finali (cittadini, imprese, altre PA, utenti interni all'Amministrazione)."

OBIETTIVO

Dare evidenza dei risultati emersi nel percorso di autovalutazione, illustrando, tra le altre cose:

- eventuali scostamenti tra la soluzione individuata in fase di autovalutazione e quella effettivamente scelta dalla Amministrazione
- il percorso e i tempi che si stima siano necessari per adottare la soluzione suggerita al termine del percorso di autovalutazione e per allinearsi a quanto previsto dalle Linee Guida

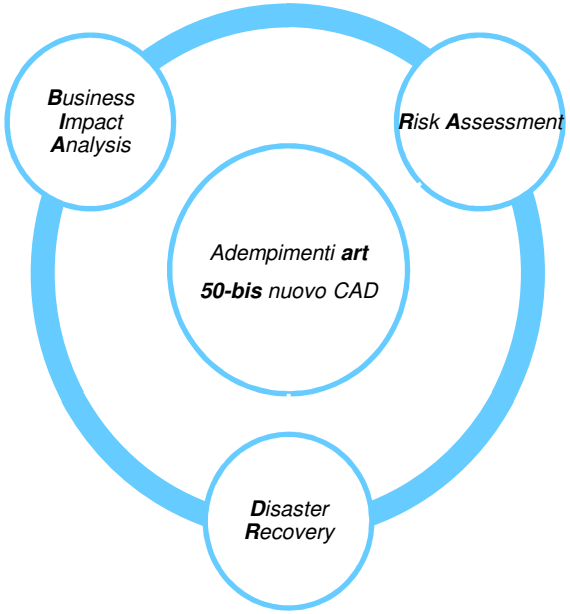
fornendo quindi a DigitPA le informazioni necessarie e propedeutiche alla realizzazione del piano di disaster recovery come parte integrante del più ampio piano di continuità operativa.

Studio di Fattibilità tecnica - Template

Analisi del contesto - perchè

PERCHÈ

"La redazione dello Studio di Fattibilità Tecnica è il momento finale di un percorso metodologico che l'Amministrazione deve effettuare"...
"senza voler prescindere dai percorsi e dalle metodologie esistenti, con particolare riguardo alla BIA e alla RA".



Analisi del contesto – contributi principali

DIMENSIONI DI IMPATTO PER LE PP.AA.

- *Aspetti economici*
- *Aspetti sociali*
- *Aspetti reputazionali*
- *Aspetti normativi*

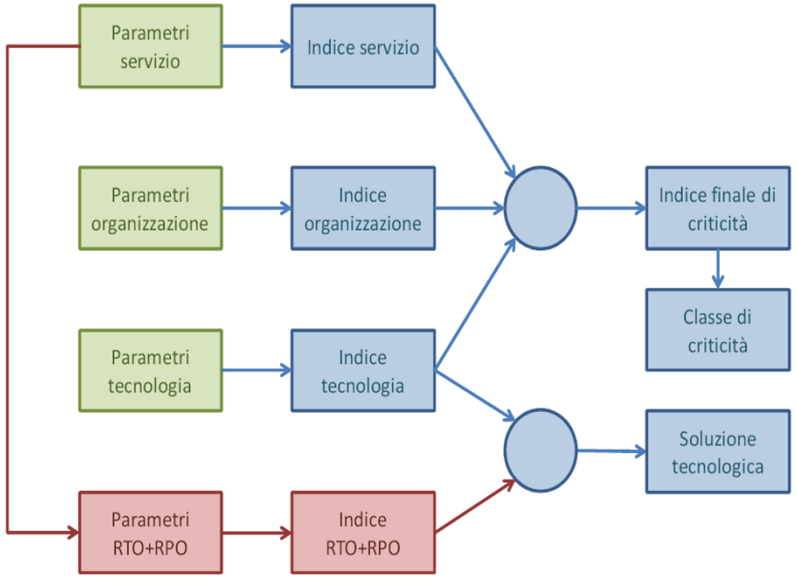
OUTPUT BIA

- *Caratterizzazione Servizi*
- *Livelli Servizio (RTO, RPO)*

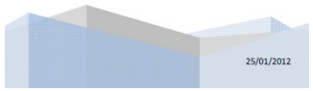
OUTPUT RA

- *Minacce in ambito*
- *Scenari di Disastro*

Autovalutazione



Studio di Fattibilità Tecnica



Agenda

- Introduzione alla Business Continuity e al Disaster Recovery
- Analisi del Contesto e degli Scenari di Disastro
- Disaster Recovery – Organizzazione e Documentazione
- La Continuità Operativa per le PP.AA.
- La Continuità Operativa in ambito bancario
- Q&A

Normativa di riferimento

*Banca d'Italia, "**Continuità operativa in casi di emergenza**", in Bollettino di Vigilanza Numero 7, **luglio 2004** in*
http://www.bancaditalia.it/vigilanza/pubblicazioni/bollvig/04/Bolvig_07_04.pdf (pagg. 7 -13)

*Banca d'Italia, "**Linee guida per la continuità di servizio delle infrastrutture qualificate dei sistemi di pagamento**", **2004**, in*
http://www.bancaditalia.it/sispaga/sms/infrastrutture/bi/linee/Linee_guida_SSP.pdf

*Banca d'Italia , "**Linee guida per la continuità di servizio dei mercati all'ingrosso e dei sistemi di supporto**", **ottobre 2004**, in*
http://www.bancaditalia.it/sispaga/sms/docum/prinstasorv/guidelines/Linee_Guida_B_C_28ottobre2004.pdf

*Banca d'Italia, "**Disposizioni di vigilanza - requisiti particolari per la continuità operativa dei processi a rilevanza sistemica**", **marzo 2007**, in*
http://www.bancaditalia.it/vigilanza/banche/normativa/disposizioni/provv/requisiti_processi_rilevanza_sistemica

*Banca d'Italia, "**Terms of Reference (ToR) per la continuità operativa**", **4 dicembre 2007**, in*
http://www.bancaditalia.it/sispaga/sms/infrastrutture/bi/tor/TOR_Business_continuityt.pdf

Definizioni

***Infrastrutture qualificate**: infrastruttura valutata tale dalla Banca d'Italia in base alle previsioni di cui al Regolamento del 24.2.2004 di attuazione dell'art. 146 TUB (artt. 1, 4.2). Ai fini delle presenti linee guida, esse ricomprendono la SIA e i Centri Applicativi Interbancari Standardizzati.*

***Piano di continuità operativa** (denominato anche **piano**): è il documento che in modo organico stabilisce, in stretto raccordo con gli obiettivi e le priorità aziendali, le regole per la gestione della continuità operativa dei diversi processi in caso di disastro su larga scala. Esso è articolato in più parti, tra loro coordinate, ciascuna riferita a un particolare settore, di rilievo per l'attività aziendale.*

***Rischio Sistemico (di regolamento):** rappresenta il rischio che un partecipante a un sistema di pagamento o a mercati finanziari, non in grado di regolare le proprie obbligazioni, determini significativi problemi di liquidità o di credito ad altri partecipanti con effetti a catena in grado di minacciare la stabilità del sistema finanziario.*

***Rischio Sistemico (di natura operativa):** rappresenta il rischio che un partecipante a un sistema di pagamento o a mercati finanziari, non in grado di eseguire o ricevere operativamente le proprie transazioni, determini significativi problemi operativi e/o di corretta determinazione delle posizioni contabili ad altri partecipanti con effetti a catena in grado di minacciare il regolare funzionamento del sistema finanziario.*

Linee Guida e Disposizioni di BdI (1/2)

Le Linee Guida forniscono i principi fondamentali cui vanno ispirati la predisposizione dei piani e degli interventi di continuità operativa.

Obiettivi di fondo sono la minimizzazione del rischio sistemico, il ripristino in tempi brevi e l'integrità delle informazioni funzionali alla rapida ripresa della normale operatività sui mercati.

Nella formulazione del piano devono trovare attenta e approfondita valutazione:
· gli scenari di rischio con le connesse analisi d'impatto;
· le soluzioni individuate riguardo alla localizzazione dei siti alternativi;
· le attività necessarie per il rispetto degli obiettivi di ripristino e ripartenza;
· le modalità di gestione e controllo del piano.

Linee Guida e Disposizioni di BdI (2/2)

Sono necessari meccanismi per acquisire e gestire regolarmente copie di riserva dei dati e del software.
Le copie devono essere conservate presso siti remoti, anch'essi dotati di un adeguato livello di protezione fisica e ambientale, coerente con i presidi previsti per il sito primario.

Più in particolare:

a) *le procedure di ripristino, accuratamente documentate e regolarmente collaudate, devono assicurare che in caso di necessità le copie siano disponibili in modo integro e tempestivo;*
b) *l'affidabilità dei supporti di memorizzazione delle copie di emergenza deve essere regolarmente verificata;*
c) *per le attività vitali e critiche devono essere conservate almeno tre "generazioni" di copie di riserva;*
d) *le attività operative devono prevedere la registrazione di archivi di log;*
e) *le procedure per la gestione di guasti devono prevedere sia l'analisi dei log, per assicurare che i guasti siano stati risolti in modo adeguato, sia la verifica delle misure correttive per assicurare che i controlli in essere non siano stati compromessi e che gli interventi siano regolarmente autorizzati.*

Requisiti di DR in ambito bancario (1/2)

Servizi infrastrutturali vitali, critici, non critici:

In termini generali, nell'area dei pagamenti sono considerati ***vitali*** *quei servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco, anche di brevissima durata, ha rilevanti effetti negativi sull'operatività degli stessi (tipici, in questo ambito, i servizi di clearing e settlement dei pagamenti wholesale, cui di norma si connette un significativo rischio sistemico di regolamento).*

I servizi ***critici*** *sono quelli che, pur assumendo particolare rilievo nell'attività dei diversi operatori, possono comunque tollerare, senza gravi inconvenienti, il blocco per alcuni giorni: in questo ambito possono collocarsi le principali procedure dei pagamenti retail, per le quali, in ragione di alcune caratteristiche strutturali del sistema dei pagamenti nazionale (ampio spessore ed elevata standardizzazione delle procedure interbancarie), si registra un significativo rischio sistemico di natura operativa per la marcata dipendenza dell'operatività degli intermediari da quella delle infrastrutture di sistema.*

I servizi ***non critici*** *sono quelli non rientranti nelle due precedenti categorie.*

Le infrastrutture qualificate definiscono la mappa delle attività correlate alla erogazione dei servizi vitali e critici, con l'indicazione dei relativi collegamenti, interni ed esterni, in termini di condizionamenti operativi, logici e temporali.

Requisiti di DR in ambito bancario (2/2)

Nel caso in cui il disastro comporti un blocco dei servizi essenziali (trasporti, energia, telecomunicazioni, ecc.) le infrastrutture qualificate devono prevedere un RTO stringente ed un RPO contenuto indicativamente entro le quattro ore precedenti la dichiarazione dello stato di crisi

Il ripristino delle attività vitali devono essere assicurate ***entro le due ore*** *dalla dichiarazione dello stato di crisi, secondo le priorità di ripartenza definite nel piano per i prelievi da ATM, stante l'importo contenuto delle transazioni, RTO potrebbe essere più stringente di RPO.*

Al contrario, in alcune procedure di trasferimento fondi – soprattutto di elevato importo si potrebbe allentare i vincoli da RTO e rendere più stressanti i termini di RPO, stante la necessità di preservare almassimo l'integrità delle transazioni.

Con riferimento al sistema TARGET, le linee fondamentali di gestione della business continuity in caso di disastro prevedono che:

a) tutti i pagamenti siano trattati nella stessa giornata contabile in cui sono immessi nel sistema e che la giornata contabile si chiuda con un ritardo massimo di due ore;

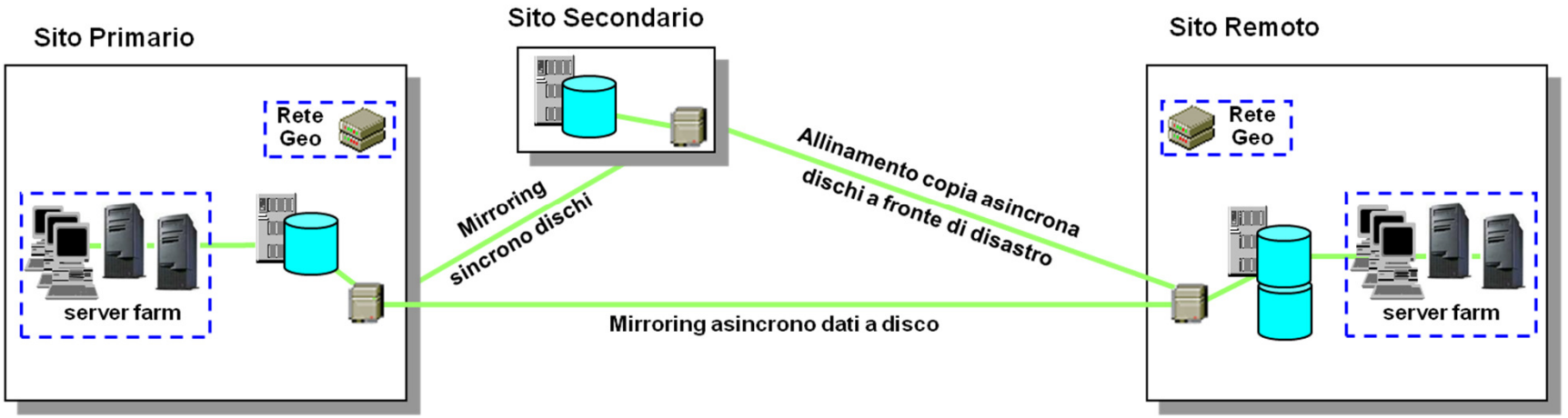
b)durante l'interruzione del servizio le Banche Centrali siano comunque in grado di trattare in modo sicuro un numero ridotto di pagamenti critici ***entro 30 minuti*** *dalla ricezione dell'ordine;*

c) l'operatività sia ripristinata presso ilsito secondario entro ***due ore*** *(non includendo il tempo necessario per i processi decisionali)*

La soluzione tecnica (1/4)

Una possibile soluzione che soddisfi i requisiti per il Disaster Recovery in ambito bancario si basa su un'architettura di remotizzazione avanzata costituita da tre siti.

- Sito Primario di Produzione
- Sito Secondario (Sito "Bunker") di replica sincrona a distanza "campus" per garantire la copia sincrona dei dati e/o eventuale 'business continuity' a distanza <60KM
- Sito Remoto (di Disaster Recovery) a distanza geografica >100KM.

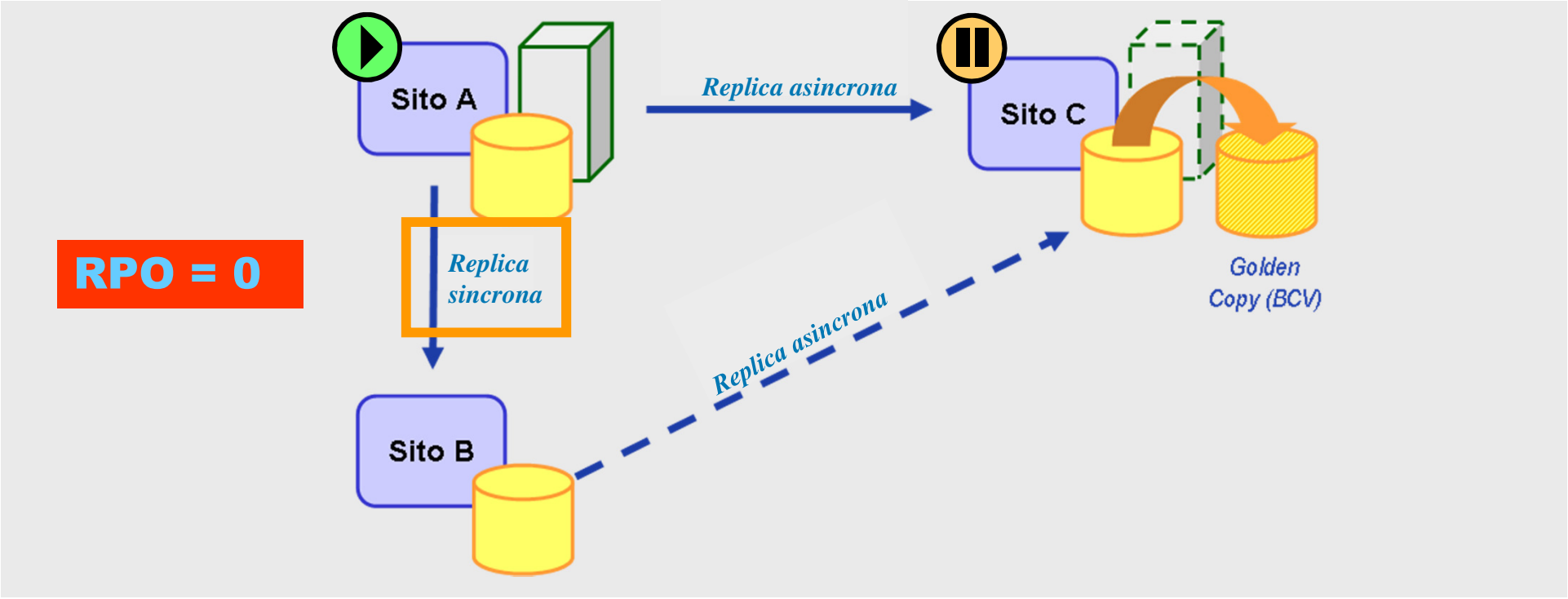


La soluzione tecnica (2/4)

- Il **Sito di produzione (A)** è la sorgente da cui vengono erogati i servizi e replicati i dati nelle normali condizioni di funzionamento del processo.
- Il **Sito bunker (B)** è dislocato a una distanza "campus" dedicato ad ospitare la replica sincrona dei dati di produzione, per mezzo di reti in fibra ottica a bassissima latenza, che garantisce il perfetto allineamento sincrono dei dati con il Sito di produzione.
  - La funzione del Sito bunker è quella di proteggere il Sito di Produzione da un disastro circoscritto al Data Center di produzione e di ripartire dal Sito Remoto con i servizi applicativi, senza perdita di dati, dopo aver eseguito il riallineamento dal Sito bunker.
- Il **Sito remoto (C)** è il Sito di Disaster Recovery, preposto al ripristino dei servizi a fronte di un evento disastroso, dislocato ad una distanza "geografica". Il Sito Remoto è collegato sia al Sito di Produzione che al Bunker. L'interconnessione viene realizzata attraverso l'utilizzo di una rete WAN in grado di trasmettere i dati in modalità asincrona e senza limitazioni di distanza.
  - La funzione del Sito Remoto è quella di proteggere il Sito di Produzione da un disastro, che può essere:
    - limitato al solo Sito di Produzione: in tal caso il Sito Remoto è in grado di garantire un RPO = 0
    - geografico, che coinvolge cioè anche il Sito bunker: in tal caso il Sito Remoto consente un RPO dell'ordine di minuti.

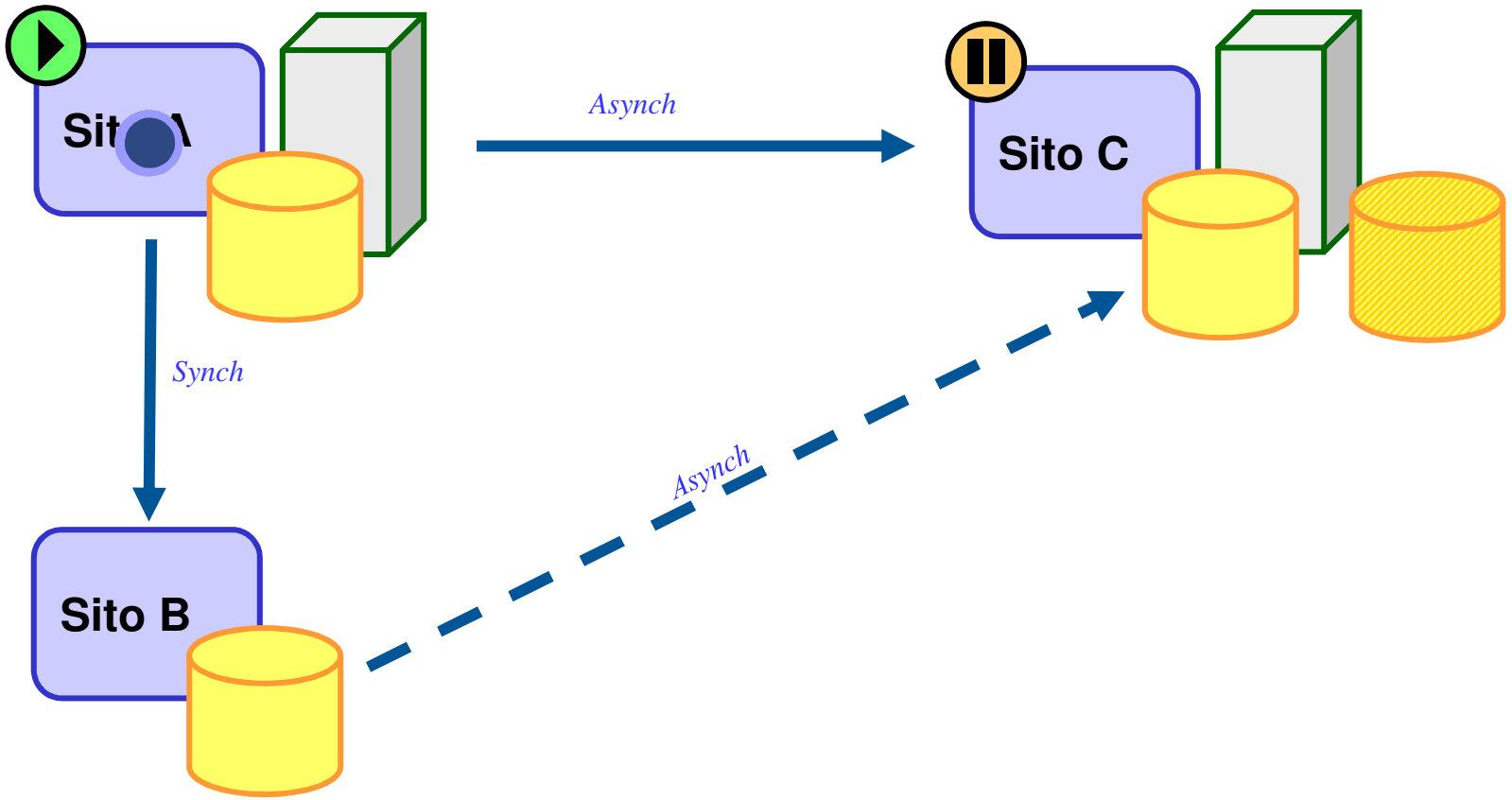
La soluzione tecnica (3/4)

- In condizioni di normale esercizio
  - dal sito primario si possono erogare tutte le funzionalità applicative;
  - dal sito secondario sono disponibili i dati allineati all'ultima transazione;
  - dal sito di DR sono disponibili i dati allineati in modalità asincrona e sistemi in stand by



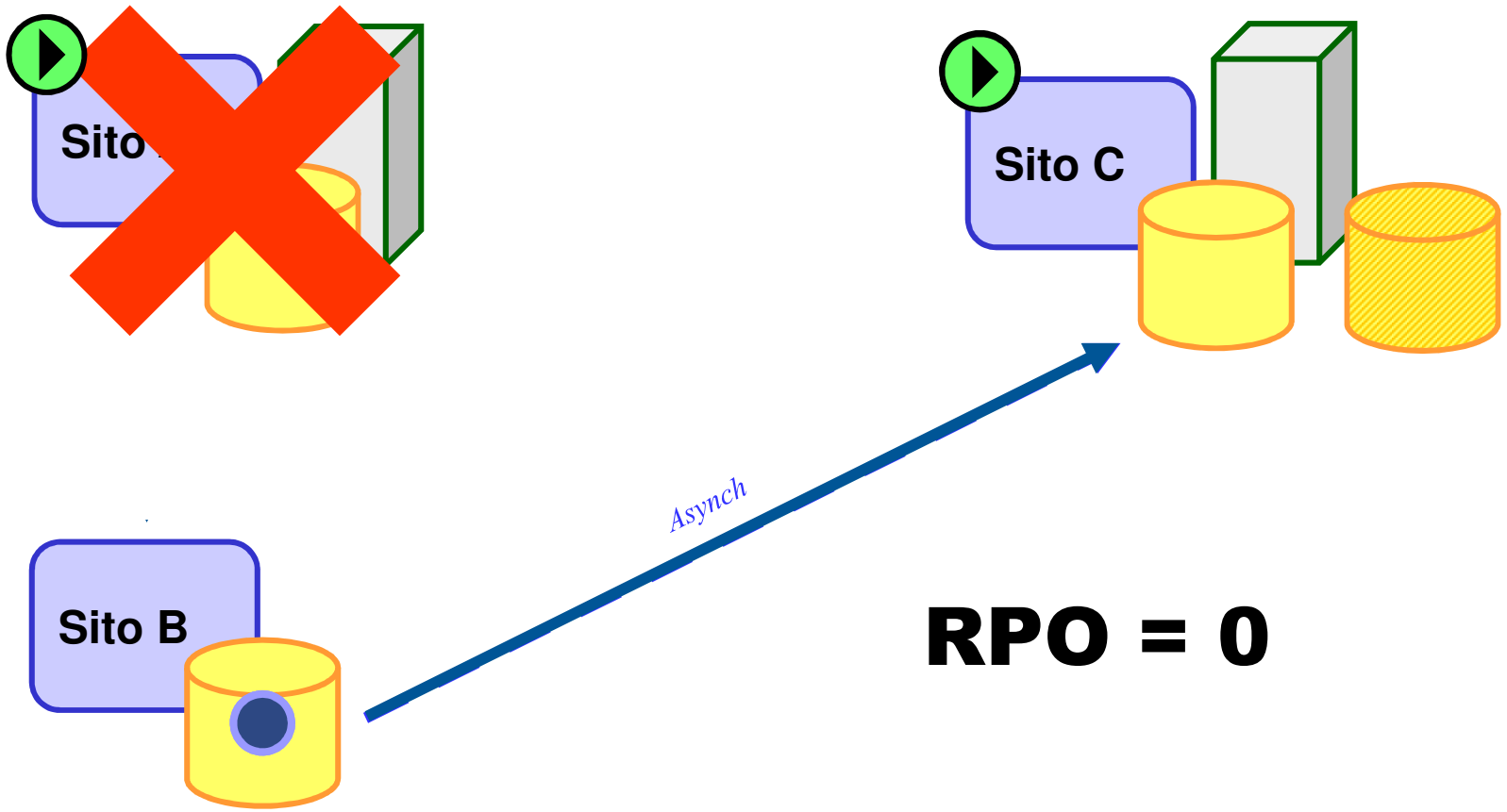
La soluzione tecnica (4/4)

- La replica **Asincrona** permette di portare i dati in modalità consistente verso il sito remoto.
- La replica **Sincrona** rende disponibile una copia consistente e aggiornata all'ultima transazione sul sito bunker.



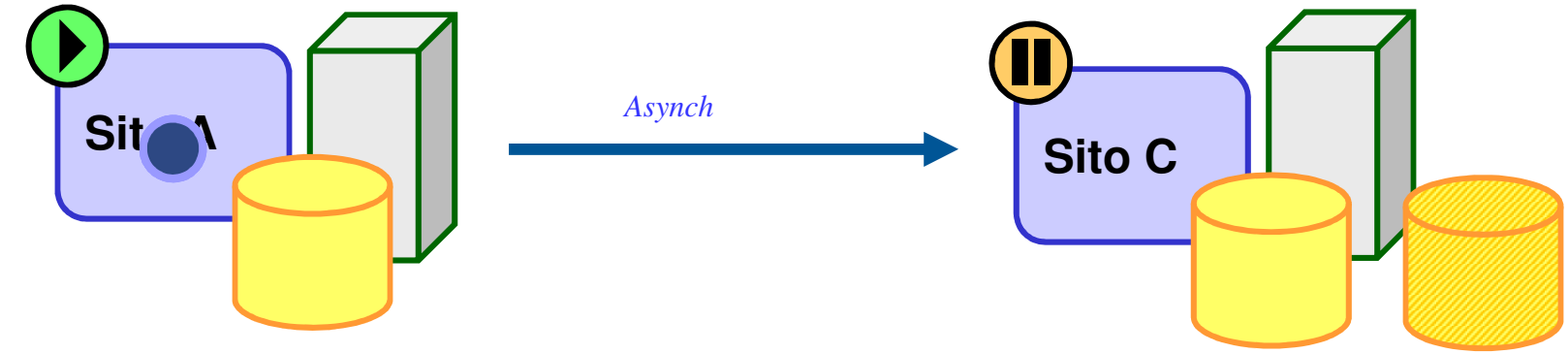
Soluzione di DR – Scenari di Disastro

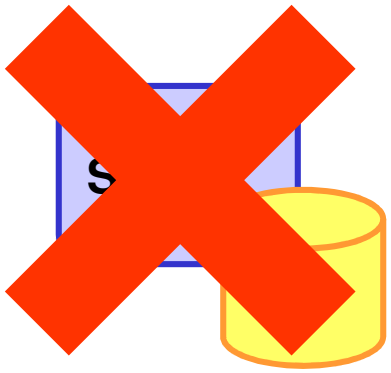
- L'**indisponibilità del sito primario** comporta l'attivazione del processo di fail over sul sito remoto mediante l'esecuzione di una sequenza di operazioni. Tale sequenza di operazioni viene attivata a valle della decisione dell'Unità di Crisi di attuare il Piano di Disaster Recovery.



Soluzione di DR – Scenari di Disastro

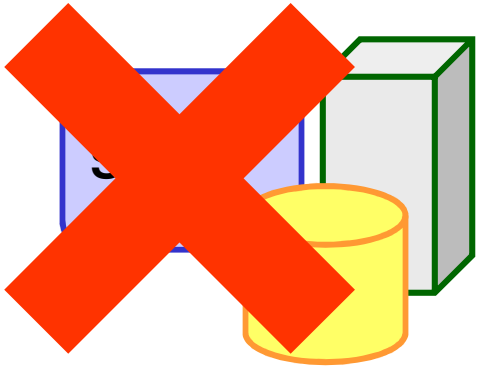
- La **indisponibilità del sito bunker** non comporta impatti significativi né sul sito di produzione né sul sito remoto.

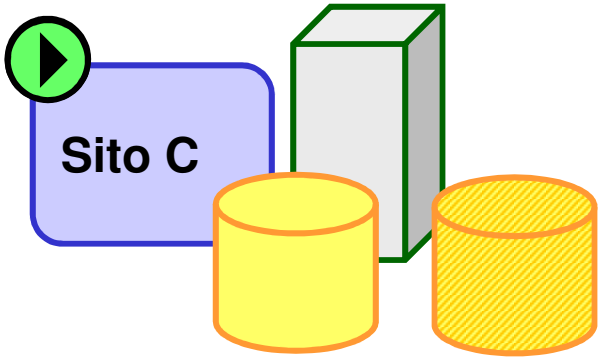


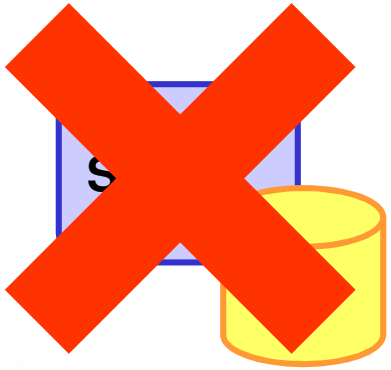


Soluzione di DR – Scenari di Disastro

- L'**indisponibilità contemporanea dei siti di produzione e bunker** rientra negli scenari di disastro che la soluzione implementata è in grado di gestire. Analogamente all'indisponibilità del solo sito secondario, l'RPO risulta dell'ordine di minuti.







RPO > 0

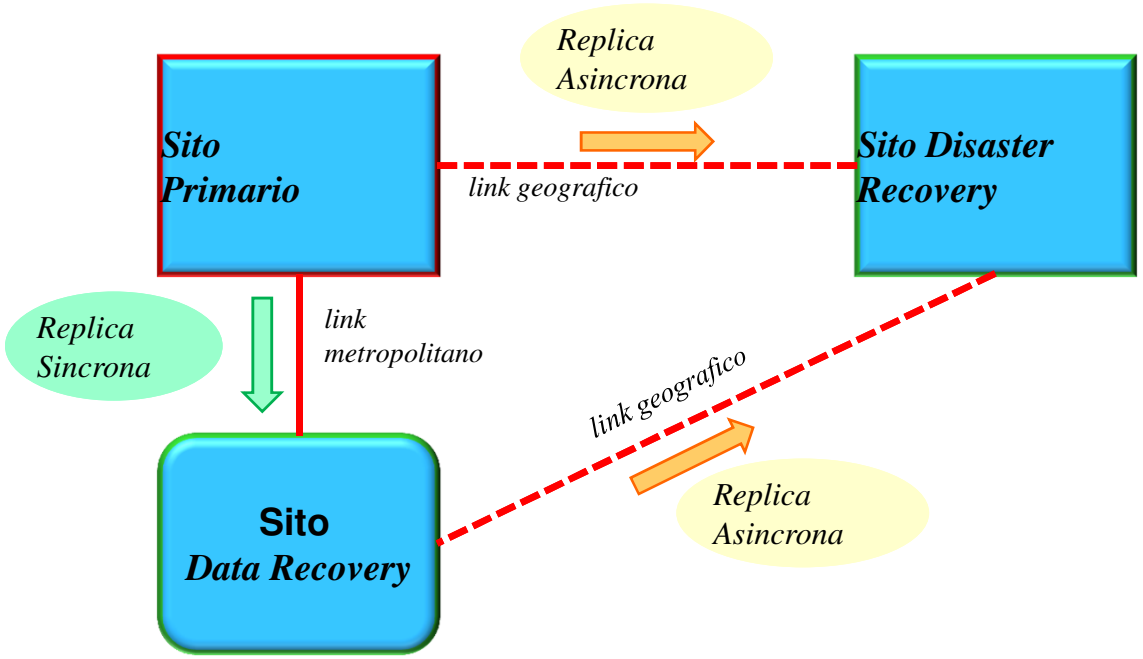
Soluzione di DR: le tecnologie abilitanti

La soluzione di disaster recovery prevede Infrastrutture IT sul Sito Primario e di DR, Sistemi di Replica Dati (hardware e software), Automazione Ripartenza Applicativi.

- **Infrastruttura IT**
  - Sito Primario, Sito secondario e Sito di Disaster Recovery
- **Sistema di Data Replication**
  - Hardware Based: soluzione di replica (a)sincrona in SAN sul (sito di DR) sito secondario.
- **Sistema di consolidamento e virtualizzazione server**
  - Disponibile per Piattaforma Intel ed AIX
- **Automatizzazione delle Procedure di DR**
  - Soluzione per la ripartenza automatizzata degli applicativi sul Sito Remoto
  - Soluzione per il monitoring automatizzato della soluzione di DR

Sistema di Data Replication

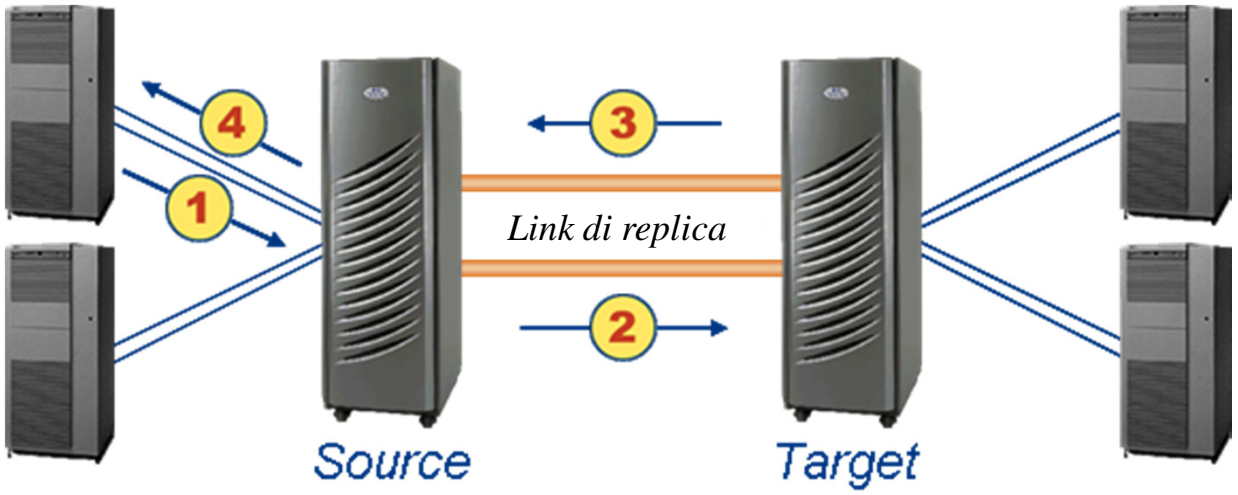
- Il sistema di Replica dei dati è stato implementato utilizzando tre tecnologie:
  - Soluzione di replica sincrona in area metropolitana
  - Soluzione di replica asincrona in area geografica
  - Soluzione di replica asincrona per la risincronizzazione geografica tra i siti di Recovery



Sistema di Data Replication

- **Replica sincrona**

1. L'operazione di scrittura viene ricevuta nelle cache dello storage Source
2. L'operazione di I/O viene trasmessa alla cache del Target
3. Un acknowledgment è inviato dal Target alla cache del Source
4. Un status di fine operazione viene presentato al server

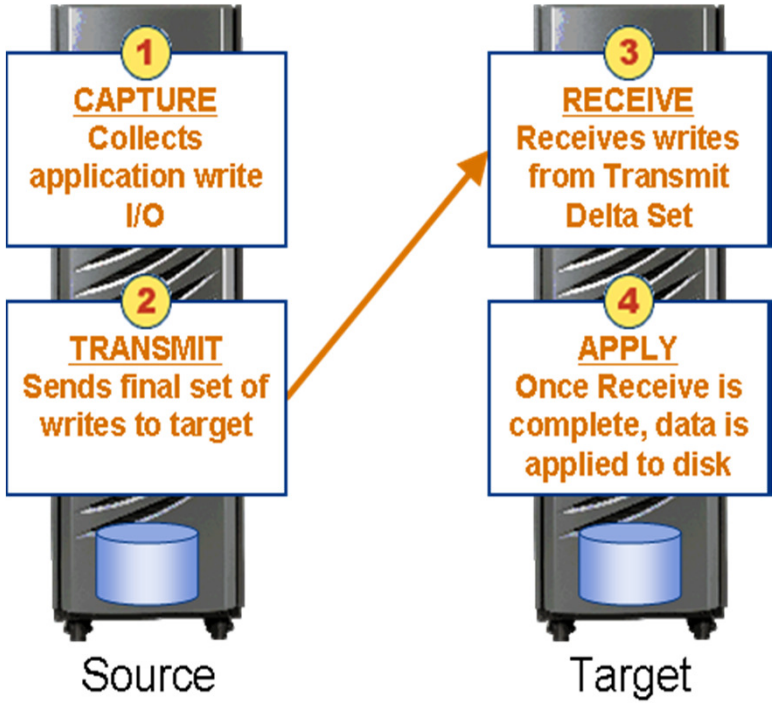


Sistema di Data Replication

- **Replica asincrona**

- Le operazioni di scrittura vengono catturate dall'unità 'Source' in cache nel (**Capture**). Al completamento del ciclo il 'Delta set' viene consolidato (**Transmit**), in modo da remotizzare sul sito secondario solo l'ultimo aggiornamento associato ad uno specifico blocco di una traccia.

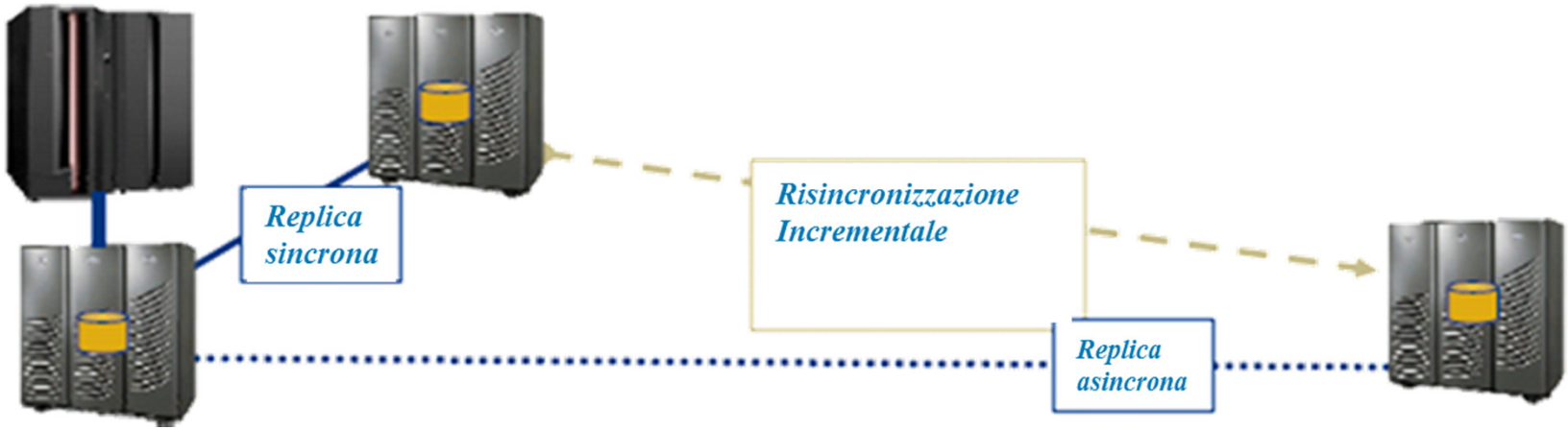
  I dati trasmessi sono ricevuti dall'unità 'Target' (**Receive**). Se la trasmissione viene completata con successo, i dati vengono promossi (**Apply**) e da qui trasferiti su disco.



Sistema di Data Replication

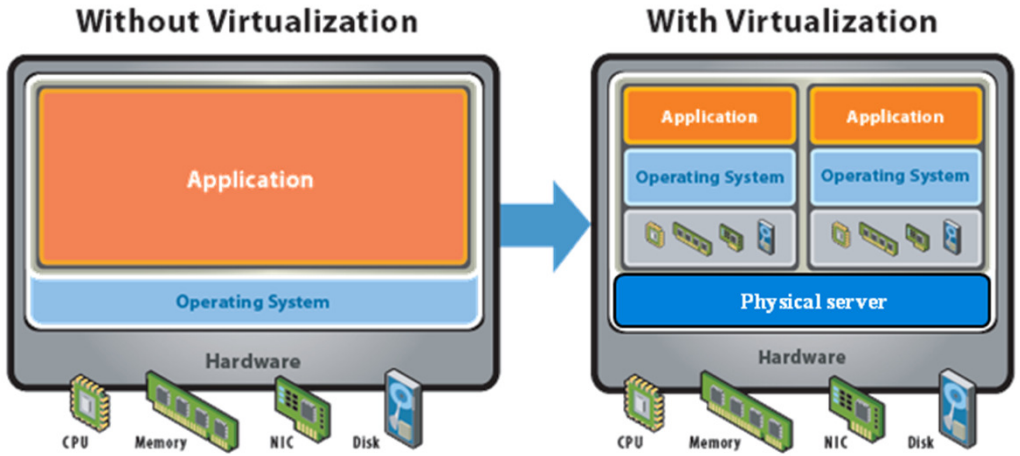
- **Replica asincrona di risincronizzazione tra i siti remoti**

  La soluzione fornisce una terza copia dei dati, completando il collegamento tra i siti non-primari (sito di Data Recovery e sito Remoto). Questa soluzione offre la possibilità di effettuare una risincronizzazione tra i due siti remoti (sito di Data Recovery e sito di Disaster Recovery) in modalità asincrona, consentendo il ripristino dei dati più recenti.



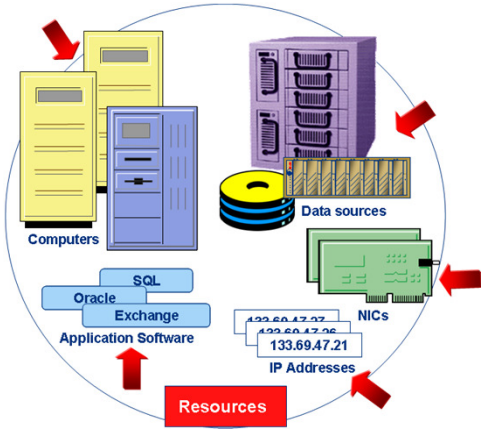
Sistema di consolidamento e virtualizzazione server

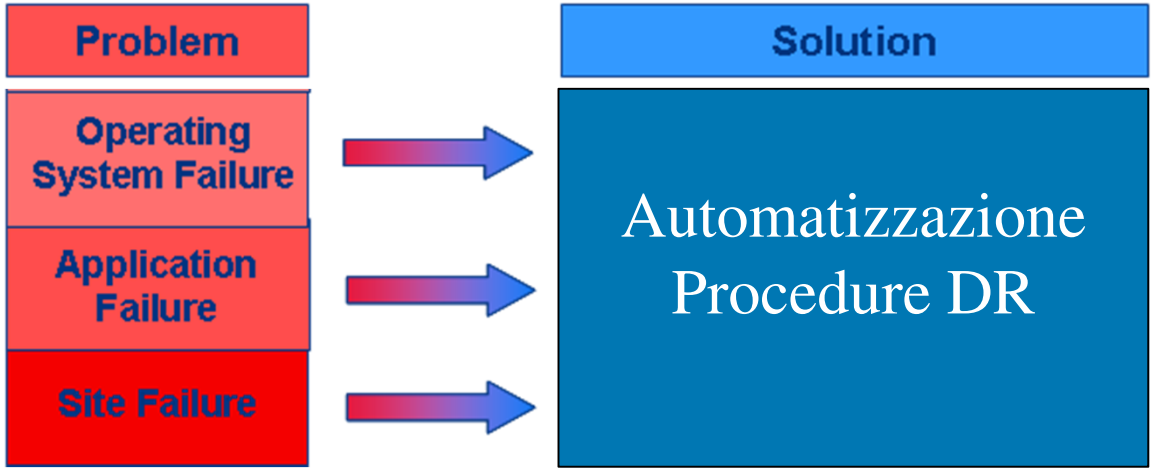
- L'architettura IT del Sito di Disaster Recovery non è speculare, come numero fisico dei server, a quella dell'ambiente del Sito di Produzione.
- Il consolidamento fisico presuppone la virtualizzazione e consente di
  - Utilizzare un numero inferiore di server per erogare gli stessi servizi senza modificare le applicazioni: il rapporto è di 1 a 4/5.
  - Muovere applicazioni, che girano su sistemi fisici dedicati, su un singolo sistema target più affidabile e più scalabile.
  - Gestire remotamente server situati in diverse locazioni semplificando quindi la loro gestione e maintenance
  - Garantire livelli di servizio utilizzando avanzate tecniche di controllo di risorse.
  - Semplificare la definizione del system monitoring e del task management
  - Incrementare la capacità della struttura dell'IT senza aggiungere nuovi sistemi.



Automatizzazione delle Procedure di DR

- Le soluzioni di automatizzazione delle Procedure di DR consentono di gestire il riavvio automatizzato di applicazioni su un sever (locale o remoto) in caso di un disservizio previsto o pianificato o di un disastro, ed eventualmente, di automatizzare il failback dei servizi, delle applicazioni e dei dati



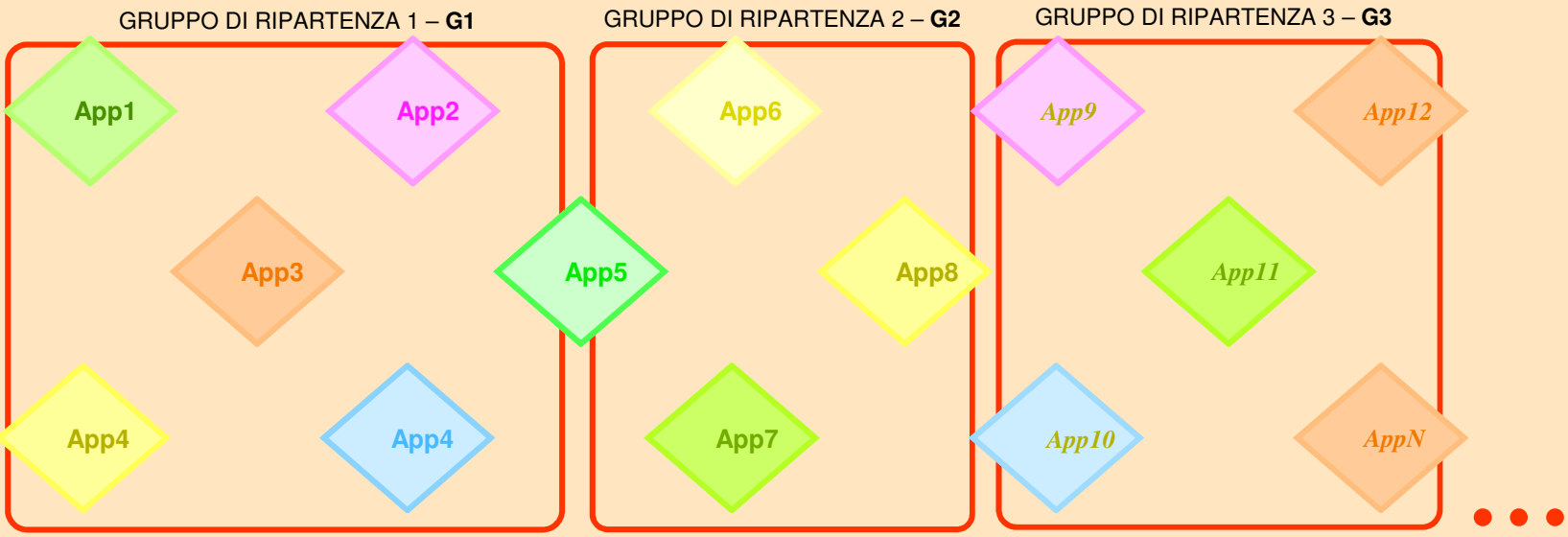


Automatizzazione Procedure DR: analisi applicativa

ANALISI per la RIPARTENZA

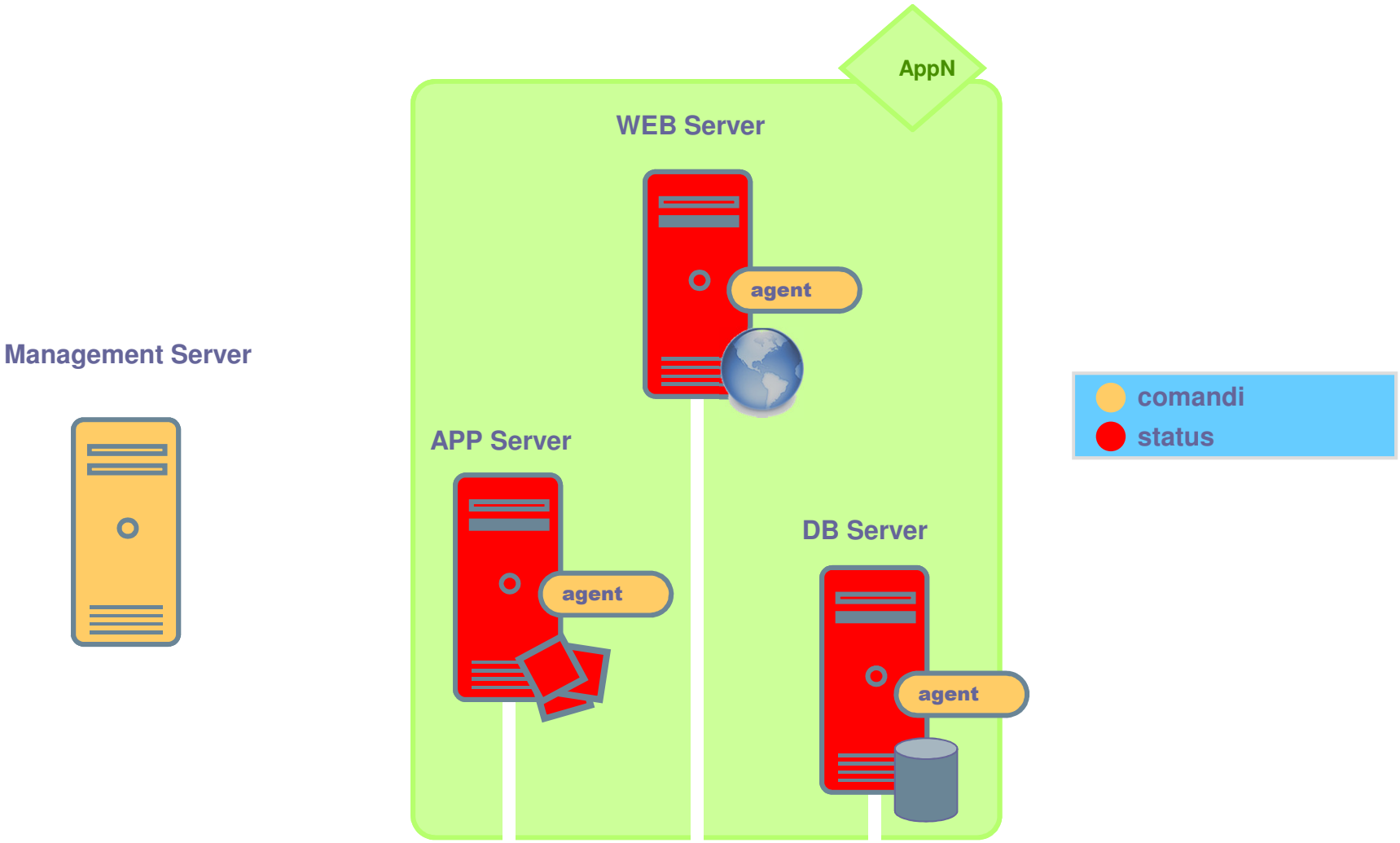
- Req. Business per DR
- Logica di Ripartenza
- Analisi Applicativa

APPLICAZIONI in AMBITO DR (lista non esaustiva):

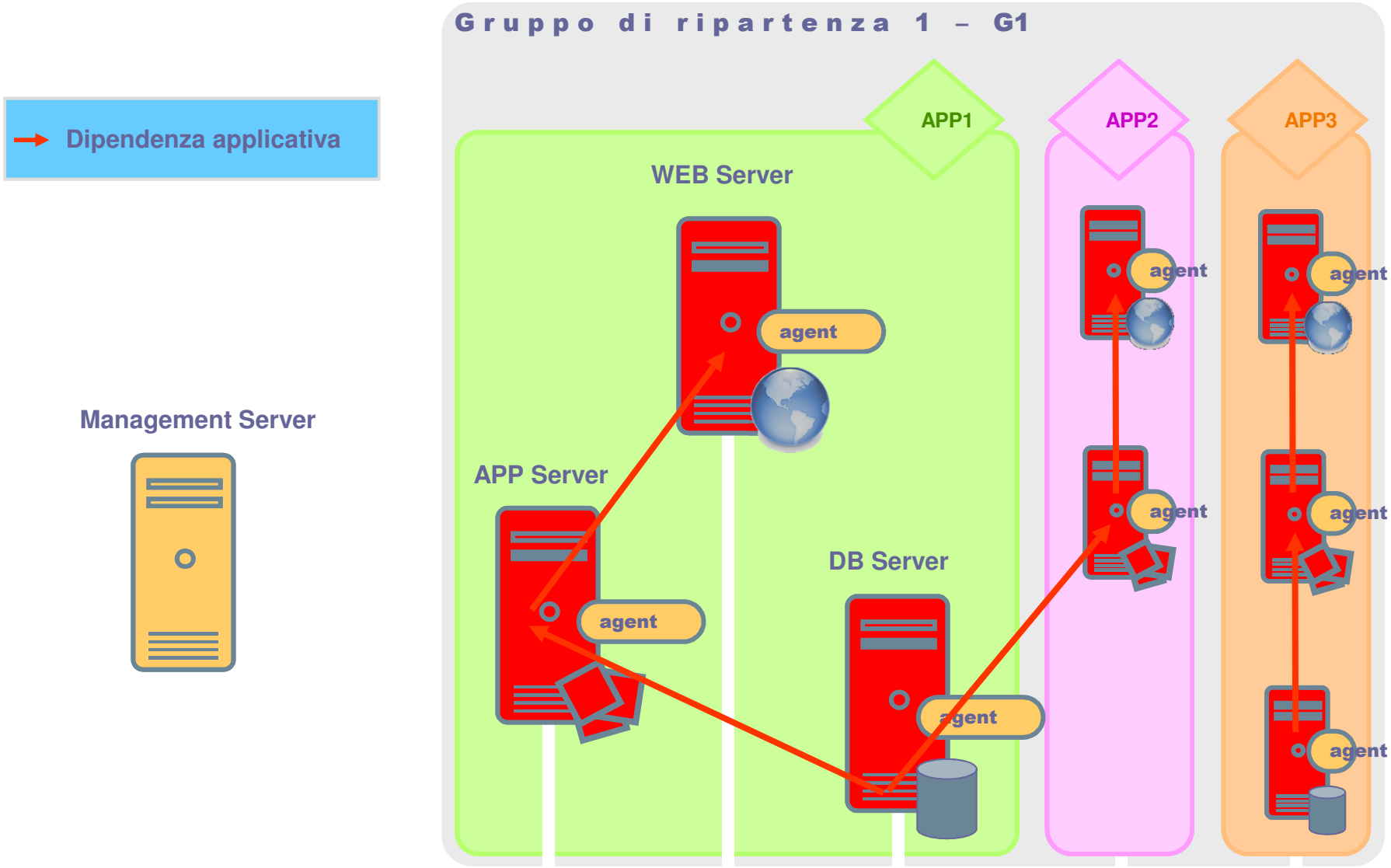


Ipotesi di raggruppamento applicativo a solo titolo di esempio

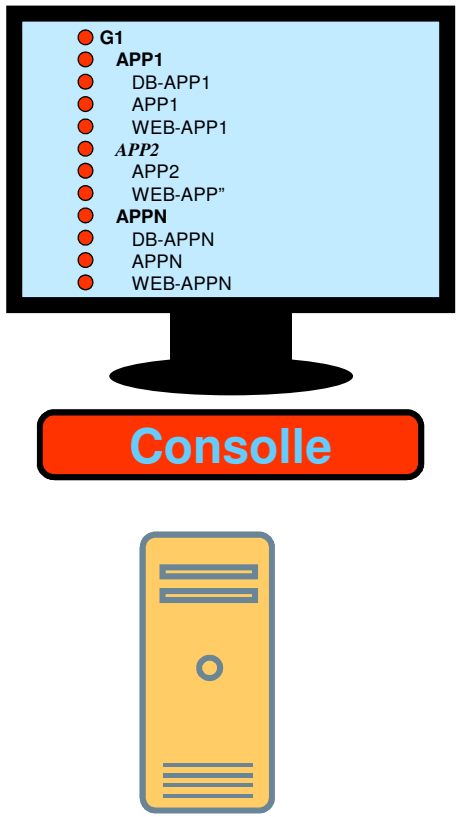
Automatizzazione Procedure DR: architettura

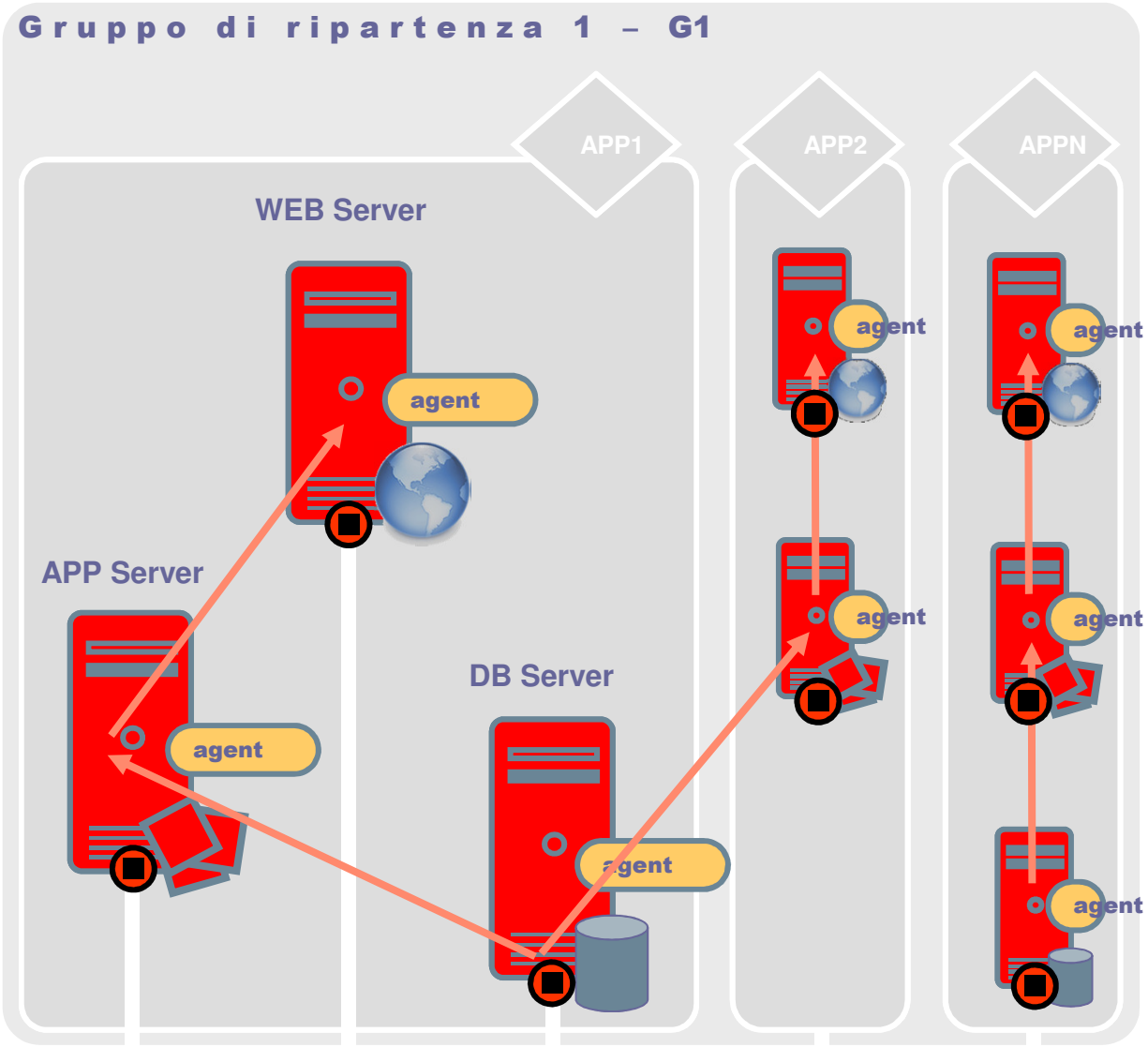


Automatizzazione Procedure DR: architettura

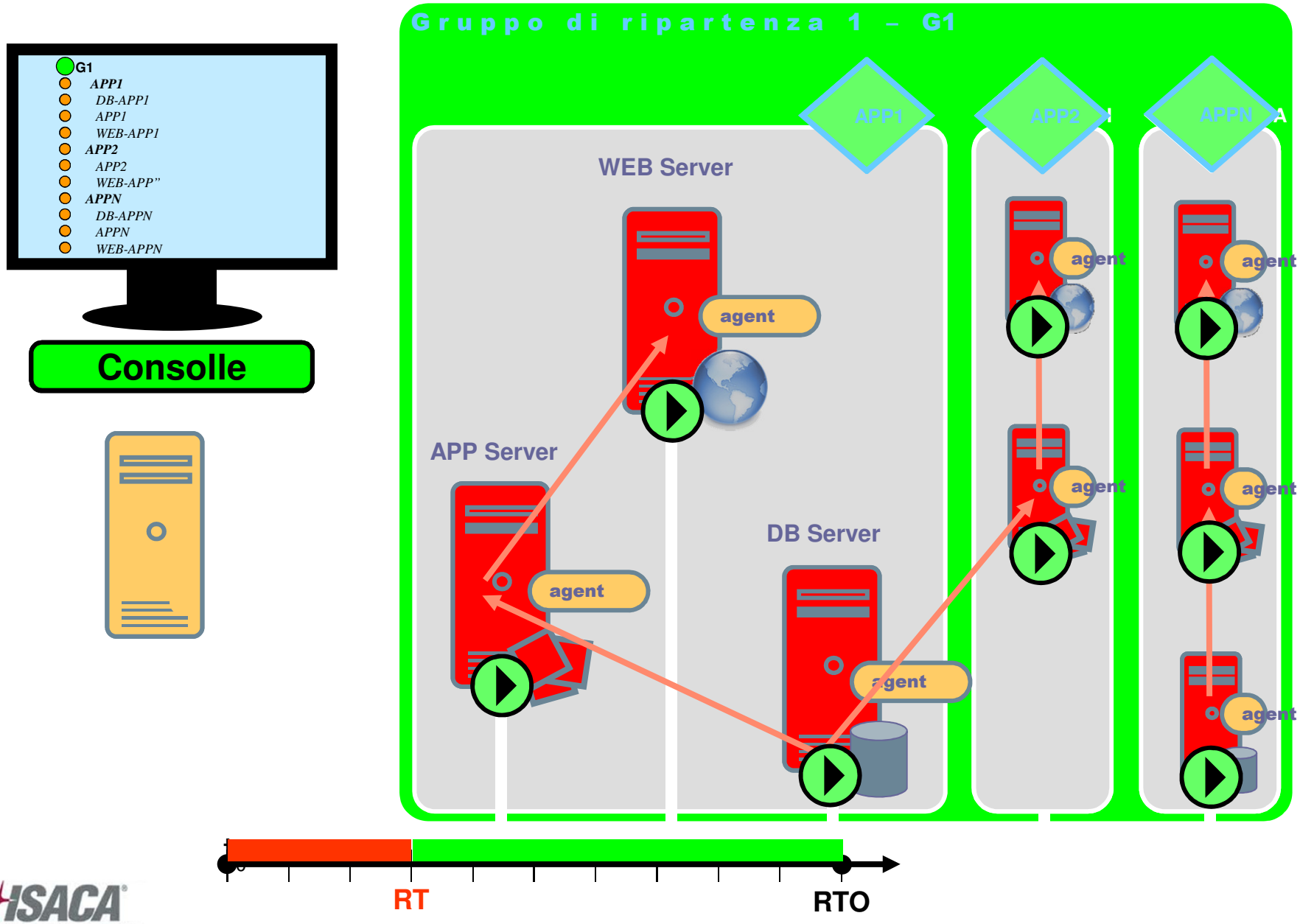


Automatizzazione Procedure DR: ripartenza applicativa





Automatizzazione Procedure DR: ripartenza applicativa



Q&A

Contatti

- benvenutich@gmail.com
- carlo.fragale@gmail.com

Grazie...