Audit sulla business continuity

Milano, 09 maggio 2016

Giancarlo Butti *(LA BS7799), (LA ISO IEC 27001:2013), CRISC, ISM, DPO*

Master di II livello in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Mi occupo di ICT, organizzazione e normativa dai primi anni 80:
•analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
•consulente in ambito documentale, sicurezza, privacy… presso aziende di diversi settori e dimensioni

Come divulgatore ho all'attivo:
• oltre 600 articoli su 20 diverse testate
• 19 fra libri e white paper, alcuni dei quali utilizzati come testi universitari
• 6 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT 2016
• membro della faculty di ABI Formazione e docente presso altre istituzioni
• relatore presso numerose sessioni di studio dell'AIEA

Sono socio e proboviro di AIEA/ISACA (www.aiea.it – Associazione Italiana Information Systems Auditors) e socio del CLUSIT (www.clusit.it – Associazione Italiana per la Sicurezza Informatica).

Partecipo ai gruppi di lavoro di ABI LAB sulla Business Continuity e Rischio informatico, di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su privacy, frodi, eidas, sicurezza dei pagamenti, di UNINFO sui profili professionali privacy.
Fra i coordinatori di www.europrivaci.info.

giancarlo.butti@promo.it

Daliso Gobbetti *(LA BS25999), (LA ISO22301)*

Laurea in Fisica, indirizzo nucleare (Università di Padova)

- *dalla fine degli 70 progettazione di sistemi in ambito universitario*
- *capo progetto nello sviluppo di applicazioni per i primi sistemi EDP destinati ad aziende di media dimensioni*
- *consulente per l'impostazione e/o la revisione dei sistemi informativi aziendali*
- *responsabile dei primi progetti di "remote banking" nel mondo bancario*

Dal 2006 ad aprile 2015 Business Continuity Manager del Gruppo Banco Popolare

daliso@tiscali.it

Programma corso: parte 1

Definizioni

Normative

Standard

Possibili soluzioni

Continuità dei servizi

Alta affidabilità / alta disponibilità

Disaster Recovery

Business continuity

Continuità dei servizi

Alta affidabilità (alta disponibilità), **disaster recovery** e **business continuity**, esprimono concetti molto diversi fra loro, anche se strettamente connessi, in quanto tutti orientati a garantire la **continuità di un servizio**.

Alta affidabilità (alta disponibilità)

Per alta affidabilità si intende la capacità di un sistema di resistere a situazioni locali di guasto, tali da consentire la continuità nell'erogazione del servizio.

L'alta affidabilità deve evitare per quanto possibile l'attivazione del Disaster Recovery

Disaster Recovery

Il Disaster Recovery è una soluzione che consente di garantire la continuità del servizio ICT nel caso di indisponibilità del sito primario

Business Continuity

La Business Continuity ha come finalità il garantire la continuità del servizio nel suo insieme, non solo della componente ICT, ma anche delle altre risorse coinvolte, quali persone, edifici, processi, documenti…

Programma corso: parte 1

Definizioni

Normativa

- **Normative di riferimento**
- **Normativa di Banca d'Italia**

Standard

Possibili soluzioni

Normative di riferimento

Decreto legislativo 30 giugno 2003, n. 196

Art. 31. Obblighi di sicurezza
1. 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.

Art. 34. Trattamenti con strumenti elettronici
1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

….

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

B. Disciplinare tecnico in materia di misure minime di sicurezza
(Artt. da 33 a 36 del Codice)

Altre misure di sicurezza

…
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Normative di riferimento

General Data Protection Regulation

Articolo 30 ***Sicurezza del trattamento***

1. Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:

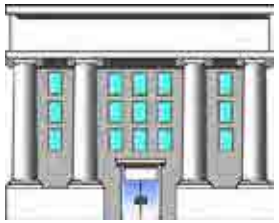
a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;

c) la capacità di ***ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico****;*

d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Normative di riferimento



Pubbliche amministrazioni

Normativa: ***CAD***

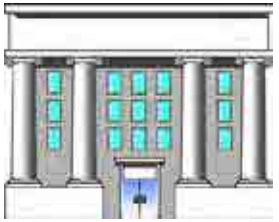
- Agenzia per l'Italia digitale: *Linee guida per il disaster recovery delle pubbliche amministrazioni (edizione 2013)*

Banche

Normativa: ***Banca d'Italia - Disposizioni di vigilanza per le banche***
(*Circolare n. 285 del 17 dicembre 2013 – 11° aggiornamento del 21 luglio 2015)*

- ABILAB: *Metodologie varie, strumenti, gruppi di lavoro, osservatorio sulla business continuity*

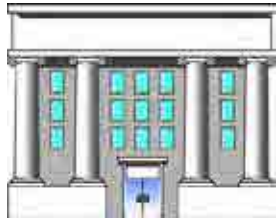
Normative di riferimento



Articolo 50-bis del CAD

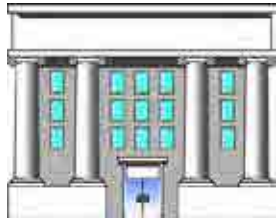
3. A tali fini, le pubbliche amministrazioni definiscono:
*a. **il piano di continuità operativa**, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;*
*b. **il piano di Disaster Recovery**, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di Disaster Recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.*

Normative di riferimento



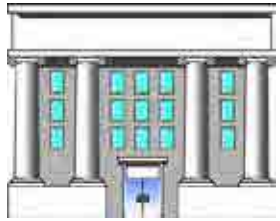
Piano di Continuità Operativa Generale dell'Organizzazione: si può definire tale il Piano che fissa gli obiettivi e i principi da perseguire da parte dell'Organizzazione; descrive i ruoli, le responsabilità, i sistemi di escalation e le procedure per la gestione della Continuità Operativa Generale (e non solo ICT) dell'Amministrazione, tenuto conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche. In realtà particolarmente complesse il Piano può essere solo un documento di primo livello cui vanno associati, per esempio, documenti di secondo livello, quali procedure relative a servizi/processi e/o sistemi specifici (per esempio il Piano di Continuità Operativa ICT) e finanche documenti di terzo livello (per esempio sotto forma di istruzioni di lavoro che riportano indicazioni operative specifiche);

Normative di riferimento



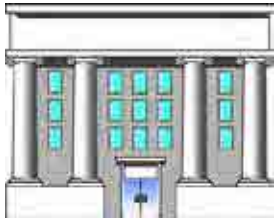
***Piano di Continuità Operativa ICT (PCO)*:** Documento operativo che descrive tutte le attività e modalità finalizzate al ripristino delle funzionalità ICT, a seguito di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi classificati come "critici"; per una realtà di dimensioni limitate, soprattutto sotto il profilo ICT, il Piano di Continuità Operativa ICT e il Piano di DR possono coincidere ma dovrà comunque essere presente la componente dedicata al Disaster Recovery. In realtà particolarmente complesse, all'opposto, il piano di continuità può essere solo un documento di primo livello, cui vanno associati, per esempio, documenti di secondo livello, quali procedure relative a servizi e/o sistemi specifici (ad esempio il Piano di Disaster Recovery) e finanche documenti di terzo livello, per esempio sotto la forma di istruzioni di lavoro che riportano le indicazioni operative specifiche;

Normative di riferimento

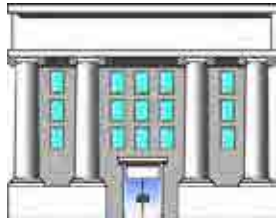


Piano di Disaster Recovery *(PDR/DRP):* Documento operativo che descrive tutte le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità delle funzioni ICT a supporto dei servizi definiti "critici", il ripristino delle stesse, entro un arco temporale predefinito, tale da rendere, il più possibile, minime le interruzioni nell'erogazione dei servizi. Si evidenzia che il PDR/DRP è la sezione del PCO che descrive le attività di ripristino del sistema informativo, costituisce parte integrante del PCO e stabilisce le misure tecniche ed organizzative per assicurare l'erogazione dei servizi classificati come critici (e delle procedure e applicazioni informatiche correlate) tramite le risorse hw, sw e di connettività presso un CED alternativo a quello/quelli di produzione;

Normative di riferimento



Normative di riferimento

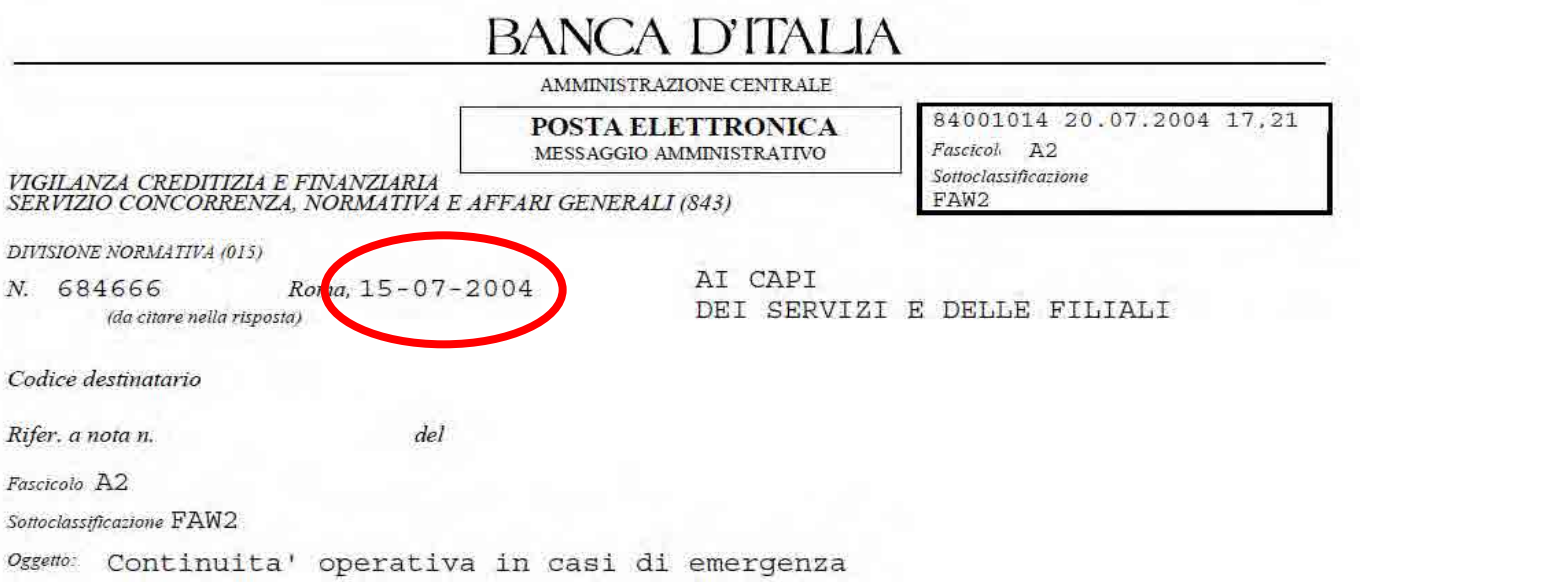


Da quanto detto consegue che la continuità dei servizi informatici rappresenta un impegno inderogabile per la PA che deve operare in modo da limitare al massimo gli effetti negativi di possibili fermi prolungati dei servizi ICT.
A titolo esemplificativo, la compromissione della continuità di un sistema informatico, può essere conseguenza di:

- errori/malfunzionamenti dei processi (il processo organizzativo che usa il servizio ICT non ha funzionato come avrebbe dovuto per errori materiali, errori nell'applicazione di norme ovvero per il verificarsi di circostanze non adeguatamente previste dalle stesse);
- malfunzionamento dei sistemi, delle applicazioni e delle infrastrutture;
- attacchi o eventi naturali di tipo accidentale;
- disastri.

Normative di Banca d’Italia

Normative di Banca d'Italia



BANCA D'ITALIA

AMMINISTRAZIONE CENTRALE

POSTA ELETTRONICA
MESSAGGIO AMMINISTRATIVO

84001014 20.07.2004 17,21
Fascicol A2
Sottoclassificazione
FAW2

VIGILANZA CREDITIZIA E FINANZIARIA
SERVIZIO CONCORRENZA, NORMATIVA E AFFARI GENERALI (843)

DIVISIONE NORMATIVA (015)

N. 684666 *Roma,* 15-07-2004
(da citare nella risposta)

AI CAPI
DEI SERVIZI E DELLE FILIALI

Codice destinatario

Rifer. a nota n. *del*

Fascicolo A2

Sottoclassificazione FAW2

Oggetto: Continuita' operativa in casi di emergenza

In relazione alla crescente complessita' dell'attivita' bancaria, all'intenso utilizzo della tecnologia dell'informazione e ai nuovi scenari di rischio, la Banca d'Italia ha attivato un complesso di iniziative volte a rafforzare i presidi di sicurezza del sistema finanziario e a promuovere lo sviluppo di piani di continuita' operativa in grado di fronteggiare crisi di ampia portata.

Normative di Banca d'Italia

BANCA D'ITALIA

ALLEGATO

Prot. n. 311014 del 23.3.2007

DISPOSIZIONI DI VIGILANZA

Oggetto: requisiti particolari per la continuità operativa dei processi a rilevanza sistemica.

Premessa

La normativa di Vigilanza sulla continuità operativa, riguardante le banche autorizzate in Italia (1), prevede la possibilità di fissare requisiti particolari, più rigorosi di quelli a carattere generale, a carico dei maggiori operatori per minimizzare il rischio di blocco del sistema finanziario italiano in caso di gravi incidenti.

A tali fini, con il presente provvedimento vengono individuati i processi ad alta criticità da proteggere ("processi a rilevanza sistemica"), sono definite le misure aggiuntive per la loro continuità operativa ("requisiti particolari") e si stabiliscono i parametri di riferimento per l'individuazione degli intermediari soggetti a tali requisiti particolari.

Normative di Banca d'Italia

Il **4 settembre 2012 la Banca d'Italia ha pubblicato un documento di consultazione** di modifica delle disposizioni di vigilanza in vigore alla data.
Le disposizioni riportate, dai contenuti estremamente ampi e variegati, contengono uno schema di disposizioni di vigilanza in materia di sistema dei controlli interni e di sistema informativo delle banche e dei gruppi bancari nonché di continuità operativa delle banche e di altri intermediari. In particolare sono inseriti capitoli che riguardano il Sistema informativo (Titolo V Capitolo 8) e la continuità operativa (Titolo V Capitolo 9).

Il documento è rimasto in consultazione alcuni mesi per raccogliere le osservazioni motivate delle banche.

Al fine di predisporre un proprio Position Paper di risposta alla consultazione, ABI ed ABILAB hanno attivato un gruppo di lavoro interno al sistema; per raccogliere i contributi è stata inviata una lettera circolare alle banche e un'informativa ai gruppi di lavoro competenti.

Normative di Banca d'Italia

Tra la fine del 2012 ed i primi mesi del 2013 si sono svolti una serie di incontri delle banche, rappresentate direttamente o per il tramite di ABI, e Banca d'Italia per illustrare le richieste di modifica/integrazione dei contenuti proposti nelle nuove disposizioni.

Alcune richieste di modifica sono state accolte (revisione degli scenari, skill del personale,…), altre respinte (possibilità di svolgimento delle prove in più anni,…).

Il tema più dibattuto ed importante è stato quello relativo alla sostituzione del RTO con il "tempo di ripristino", stabilendo che questo tempo venga conteggiato a partire dalla dichiarazione dello stato di crisi, e non dal momento dell'interruzione del servizio.

In ogni caso Banca d'Italia ha fornito la propria valutazione e le motivazioni delle scelte effettuate, consentendo anche di comprendere meglio il significato delle decisioni prese.

Normative di Banca d'Italia

Comunicato Stampa

DIFFUSO A CURA DEL SERVIZIO SEGRETERIA PARTICOLARE

Roma, 3 luglio 2013

Nuove disposizioni di vigilanza prudenziale per le banche

La Banca d'Italia comunica che sono state aggiornate le disposizioni di vigilanza prudenziale per le banche in materia di **sistema dei controlli interni, sistema informativo e continuità operativa**.

La nuova disciplina costituisce un quadro normativo organico e coerente con le migliori prassi internazionali e con le raccomandazioni dei principali *organismi internazionali* e si ispira ad alcuni **principi di fondo**: il coinvolgimento dei vertici aziendali; la visione integrata dei rischi; l'efficienza e l'efficacia dei controlli; l'applicazione delle norme in funzione della dimensione e della complessità operativa delle banche.

Nuove disposizioni di vigilanza prudenziale per le banche

Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013

Normative di Banca d'Italia

Principi di fondo della normativa:

- **coinvolgimento vertici** aziendali
- **visione integrata** dei **rischi**
- **efficienza ed efficacia dei controlli**
- applicazione delle norme in **funzione** della **dimensione e** della **complessità operativa**

Principali elementi di novità:

- Definizione di **compiti e responsabilità** degli **organi** aziendali con funzione di **supervisione strategica**, **gestione** e **controllo**.
- Introduzione di una disciplina in materia di **esternalizzazione** delle **funzioni aziendali** e del **sistema informativo**
- Con riferimento al **capitolo 9 sulla continuità operativa**, la **normativa riorganizza le disposizioni** attualmente contenute in diverse fonti (circolari del 2004 e 2007) **in un unico titolo del documento**, introducendo le seguenti novità:
  - ridefinisce le modalità di **gestione delle crisi** all'interno del sistema finanziario, definendo il processo di escalation
  - formalizza il **ruolo del CODISE**, quale struttura di coordinamento presieduta da Banca d'Italia

Normative di Banca d'Italia

Disposizioni di vigilanza per le banche

Circolare n. 285 del 17 dicembre 2013

Circolare n. 285: "Sistema dei controlli interni, Sistema informativo, Continuità operativa e Governo e gestione del rischio di liquidità" – 11° Aggiornamento del 21 luglio 2015.

1. Premessa

Il presente aggiornamento introduce nella Parte Prima, Titolo IV della Circolare n. 285 del 17 dicembre 2013 i Capitoli 3 (Sistema dei controlli interni), 4 (Sistema informativo), 5 (Continuità operativa) e 6 (Governo e gestione del rischio di liquidità), prima contenuti nella Circolare n. 263 del 27 dicembre 2006 ([1]). In questo modo, prosegue l'obiettivo di semplificare e razionalizzare la normativa di vigilanza, facendola progressivamente confluire in un'unica circolare.

Normative di Banca d'Italia

Dall'entrata in vigore del presente aggiornamento, sono abrogate le seguenti disposizioni contenute nel Titolo V della Circolare n. 263 del 27 dicembre 2006:

- Capitolo 2 - Governo e gestione del rischio di liquidità;
- Capitolo 7 - Sistema dei controlli interni;
- Capitolo 8 - Sistema informativo;
- Capitolo 9 - Continuità operativa.

Nel fare riserva di pubblicare una ristampa integrale della circolare, si fa presente che i riferimenti contenuti nelle vigenti disposizioni ai capitoli della Circolare n. 263 abrogati con il presente aggiornamento devono intendersi riferiti ai nuovi Capitoli introdotti nella Circolare n. 285 con il medesimo aggiornamento.

Normative di Banca d'Italia

Nell'ambito della normativa 285 la Continuità Operativa è trattata nella Parte Prima, Titolo IV, Capitolo numero 5, ma richiami a questo ambito sono presenti anche nel Capitolo 4 – Il sistema informativo Sezione IV – **La gestione della sicurezza informatica**

Normative di Banca d'Italia

alta affidabilità/disponibilità

— *in relazione alle esigenze di disponibilità delle singole applicazioni, sono definite procedure di backup (di dati, software e configurazione) e di ripristino su sistemi alternativi, in precedenza individuati;*

— *le architetture sono disegnate in considerazione dei profili di sicurezza informatica delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario valuta la necessità di predisporre piattaforme particolarmente robuste e ridondate (ad es., applicando il principio del no single point of failure) volte a garantire l'alta disponibilità delle applicazioni maggiormente critiche, in sinergia con le procedure e il sistema di disaster recovery;*

— *in funzione dei profili di rischio delle comunicazioni, delle applicazioni e dei servizi acceduti, i collegamenti telematici interni alla banca o al gruppo sono opportunamente ridondati; in relazione al rischio di incidenti di sicurezza informatica che possono determinare l'interruzione dei servizi (ad es., mediante attacchi di tipo denial of service o distributed denial of service), oltre a soluzioni specifiche per l'individuazione e il blocco del traffico malevolo, la banca valuta l'opportunità di sfruttare procedure e strumenti per l'allocazione dinamica di capacità trasmissiva ed elaborativa;*

Normative di Banca d'Italia

Come accennato in precedenza nella normativa 285 la Continuità Operativa è trattata nella Parte Prima, Titolo IV, Capitolo numero 5 che si divide in **4 paragrafi, che trattano i seguenti aspetti:**

- i **destinatari della disciplina, rimandando all'allegato per quanto riguarda le** disposizioni in senso stretto;
- le **fonti normative che regolano la materia;**
- banche soggette ai **requisiti applicabili a tutti gli operatori** (**sezione II dell'allegato);**
- banche soggette ai **requisiti particolari per i processi a rilevanza sistemica** (**sezione III dell'allegato).**

Normative di Banca d'Italia

ALLEGATO A, SEZIONE I – DISPOSIZIONI DI CARATTERE GENERALE

DEFINIZIONI

Sono state **introdotte** le definizioni di:

- *CODISE*
- *crisi*
- *escalation*
- *Emergenza*

È stato eliminato il riferimento ai concetti di RTO e RPO all'interno del documento, introducendo la definizione di *tempo di ripristino di un processo:*

" periodo che intercorre fra il momento in cui l'operatore dichiara lo stato crisi e l'istante in cui il processo è ripristinato a un livello di servizio predefinito. Esso è costituito dai tempi di:

- *analisi degli eventi e decisione delle azioni da intraprendere, prima di effettuare gli interventi;*
- *ripartenza del processo, attraverso l'attuazione degli interventi tecnici e organizzativi e la successiva verifica sulla possibilità di rendere nuovamente disponibili i servizi senza danni e in condizioni di sicurezza."*

Normative di Banca d'Italia

DEFINIZIONI

Sono state **riprese** le precedenti **definizioni** di:

- *gestione della continuità operativa*
- *piano di disaster recovery*
- *piano di continuità operativa*

A quest'ultima definizione sono state apportate le seguenti modifiche:

"documento che formalizza i principi, fissa gli obiettivi, descrive le procedure ***e individua le risorse****, per la gestione della continuità operativa dei processi aziendali critici* ***e a rilevanza sistemica. Esso è generalmente articolato in piani settoriali;"***

in seguito, nel paragrafo dedicato alla **responsabilità del piano di continuità operativa**(3.3), si prevede che

"Laddove il piano di continuità operativa sia articolato in piani settoriali, gli operatori individuano i referenti per ciascuno di essi. I referenti dei piani settoriali (1) coordinano, per gli aspetti di competenza, i lavori…"

Rispetto alla normativa precedente, sono quindi stati **esplicitamente individuati i piani settoriali** (**e i relativi referenti**) che potrebbero formare il piano di c.o.

Normative di Banca d'Italia

AMBITO DEL PIANO DI CONTINUITÀ OPERATIVA

In relazione agli **scenari di crisi** che prende in considerazione il piano di continuità operativa, è stato esplicitato che i **fattori di rischio** che generano tali scenari **derivano da eventi naturali o dall'attività umana** (comprendendo quindi anche il caso di **danneggiamenti gravi provocati da dipendenti**).

Tra gli scenari di crisi sono stati separati i casi di

- *indisponibilità di sistemi informativi critici*
- *alterazione o perdita di dati e documenti critici.*

Nella versione precedente delle disposizioni, il testo citava la possibilità di "*alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche*", con il rischio di **limitare l'indisponibilità dei sistemi ICT** al solo evento di **attacchi** provenienti dall'**esterno**.

È stata inoltre inserita la seguente previsione:

Il piano di continuità operativa indica le procedure per il rientro dall'emergenza, con particolare attenzione alla rilevazione dei danni, alla gestione di tutte le operazioni di rientro, alla verifica dell'operatività per i servizi ripristinati.

dettagliando quindi maggiormente i **contenuti** del **piano di continuità operativa**.

Normative di Banca d'Italia

L'organo di amministrazione

- *approva il piano* ***di continuità operativa e le successive modifiche a seguito di adeguamenti tecnologici ed organizzativi, accettando i rischi residui non gestiti dal piano di continuità operativa***
- *è informato, con frequenza almeno annuale, sugli* ***esiti dei controlli*** *sull'adeguatezza del piano* ***nonché delle verifiche delle misure di continuità operativa***
- *promuove* ***lo sviluppo, il controllo periodico del piano di continuità operativa e*** *l'aggiornamento dello stesso a fronte di…*
- *approva il piano annuale delle verifiche delle misure di continuità operativa ed esamina i risultati delle prove* ***documentati in forma scritta.***

L'organo con funzione di controllo *(collegio sindacale, il consiglio di sorveglianza o il comitato per il controllo sulla gestione)*

- *ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del piano di continuità operativa.*

Normative di Banca d'Italia

I processi critici

*"i processi **relativi a funzioni aziendali di particolare rilevanza che, per l'impatto dei** danni conseguenti alla loro indisponibilità, necessitano di elevati livelli di continuità operativa…"*

*"Il responsabile del processo **individua**, in accordo con gli indirizzi strategici e con le regole stabilite nel piano di continuità operativa**, il tempo di ripristino del processo** e collabora attivamente alla realizzazione delle misure di continuità operativa"*

La responsabilità del piano di continuità operativa

*"**il responsabile** cura lo sviluppo del piano di continuità operativa, **ne assicura l'aggiornamento nel continuo**, a fronte di cambiamenti organizzativi o tecnologici rilevanti, e ne verifica l'adeguatezza, con cadenza almeno annuale. Tale figura tiene inoltre i contatti con la Banca d'Italia in caso di crisi."*

Normative di Banca d'Italia

Il contenuto del piano di continuità operativa

*"Sono previste **misure di escalation rapide** che consentano, una volta assunta consapevolezza della portata dell'incidente, di dichiarare lo stato di crisi in tempi brevi.*
***I processi** per la **gestione degli incidenti** e per la **dichiarazione e gestione dello stato di crisi** sono **formalizzati e strettamente integrati** fra loro."*

Con riferimento ai **sistemi informativi** centrali e periferici, è stato chiarito che il **piano di continuità operativa integra il piano di disaster recovery**. Inoltre:

*"La frequenza dei back-up è correlata **alle dimensioni e alle funzioni** dell'operatore"* , facendo **riferimento alla dimensione della banca**, piuttosto che al volume di operatività (**precedente normativa**); inoltre

*"gli archivi di produzione **dei processi critici** sono duplicati almeno giornalmente*."

Normative di Banca d'Italia

Le verifiche

*"Con frequenza almeno annuale **sono svolte verifiche complessive**, basate su scenari il più possibile realistici, …"*

*"Le prove sono **preferibilmente** realizzate con dati di produzione."*

Le risorse umane

*Le procedure di continuità operativa sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse **non impegnate nell'ordinaria attività nei processi cui si riferiscono**.*

Controlli

*In caso di incidenti, la **funzione di audit verifica la congruità dei tempi rilevati** per la dichiarazione dello stato di crisi.*

Normative di Banca d'Italia

ABISERVIZI ABI FORMAZIONE

3.7 Esternalizzazione, infrastrutture e controparti rilevanti

In caso di esternalizzazione di funzioni aziendali connesse allo svolgimento di processi critici, il piano di continuità operativa prevede le misure da attuare in caso di crisi con impatto rilevante sull'operatore o sul fornitore di servizi.

Nel contratto sono formalizzati i livelli di servizio assicurati in caso di crisi e le soluzioni di continuità operativa poste in atto dal fornitore di servizi, adeguati al conseguimento degli obiettivi aziendali e coerenti con le prescrizioni della Banca d'Italia. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.

L'operatore acquisisce i piani di continuità operativa del fornitore di servizi o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità operativa realizzate all'interno. Il fornitore di servizi comunica

BANCA D'ITALIA

11° aggiornamento

Circolare n. 285 del 17 dicembre 2013

Parte Prima.IV.5.10

Normative di Banca d'Italia

Esula dalle finalità del corso

ALLEGATO A, SEZIONE III – REQUISITI PARTICOLARI PER I PROCESSI A RILEVANZA SISTEMICA

Tra i servizi erogati dai ***processi a rilevanza sistemica***, sono state effettuate le seguenti ***integrazioni***:

- *servizi di pagamento al dettaglio a larga diffusione tra il pubblico. Sono inclusi: bollettini postali, pagamento delle pensioni sociali,* ***erogazione del contante****;*
- *servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco ha rilevanti effetti negativi sull'operatività degli stessi. Sono inclusi: gestione delle infrastrutture telematiche per l'erogazione del contante tramite terminale ATM, supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati" (SITRAD).*

Rispetto alla normativa precedente, è stato formalizzato il ruolo del CODISE, quale struttura di coordinamento presieduta da Banca d'Italia. È stato indicato che ***le banche alle quali si applicano i requisiti particolari*** di continuità operativa***, sono individuate nominativamente da Banca d'Italia***

"partecipano alle iniziative per il coordinamento della continuità operativa del sistema finanziario del CODISE."

Programma corso: parte 1

Definizioni

Normativa

Standard

Standard di riferimento

Cobit 5

ISO 22301

Possibili soluzioni

Standard

Standard ISO relativi alla continuità operativa generale dell'organizzazione:
ISO 22313 e ISO 22301 – sistema di gestione della CO generale

Standard ISO/IEC relativi alla CO e al DR ICT
ISO/IEC 27031 relativo alla CO ICT
ISO/IEC 24762 relativo ai servizi di DR ICT

Standard ISO/IEC relativi a tematiche ICT correlate alla CO e al DR
ISO/IEC 27001 e 27002 relative alla sicurezza ICT che prevedono tra gli oggetti di controllo la gestione della continuità operativa
ISO/IEC 20000-1 e 20000-2 relative al sistema di gestione dei servizi ICT che include
tra i servizi la gestione della continuità dei servizi

Standard

ISO 22301

(“Societal security -- Business continuity management systems – Requirements”)

emesso nel maggio 2012 tratta del sistema di gestione della CO e delle verifiche, che implica un percorso di certificazione

ISO 22313

(“Societal security. Business continuity management systems. Guidance”)

emesso nel dicembre 2012, descrive le buone pratiche in materia di CO.

Costituisce una guida per la ISO 22301, aiutando le organizzazioni che intendono realizzare efficaci sistemi di gestione della CO.

Standard

ISO/IEC 24762

("Information technology — Security techniques — Guidelines for information and communications technology Disaster Recovery services") copre i seguenti aspetti:

messa in opera, gestione, supervisione e manutenzione delle infrastrutture e dei servizi per il Disaster Recovery;

le esigenze per la fornitura dei servizi e delle infrastrutture del Disaster Recovery;

i criteri di selezione dei siti alternativi;

le attività per il miglioramento continuo dei servizi e delle prestazioni del Disaster Recovery.

Standard

ISO/IEC 27031

("Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity")

Il campo di applicazione dello standard norma ISO / IEC 27031:2011 comprende tutti gli eventi (tra cui quelli correlati alla sicurezza), che potrebbero avere un impatto sulle infrastrutture e sistemi ICT e include ed estende la pratica della gestione dei problemi della sicurezza delle informazioni e la gestione e la disponibilità dei servizi ICT.

Lo standard fornisce un collegamento tra gestione generale della continuità operativa e delle tecnologie dell'informazione, fornendo una visione che mette insieme BS 25999, ISO/IEC 24762 e ISO 27001. Lo standard dà quindi un quadro di riferimento e dei metodi di processo di identificazione e di specificazione di tutti gli aspetti per migliorare la preparazione dell'ICT dell'organizzazione alle emergenze, garantendo quindi la continuità dell'organizzazione stessa.

Standard

ISO/IEC 27002

(“Information technology -- Security techniques -- Code of practice for information security management”)

è uno dei primi standard dedicati alla sicurezza informatica sotto il profilo dei processi. Lo standard contiene raccomandazioni concrete per garantire la sicurezza delle informazioni, più precisamente il processo di messa in sicurezza. Comprende nove capitoli che trattano i differenti aspetti riguardanti la sicurezza.

Il capitolo 14 dello standard 27002 tratta della “gestione del piano di continuità dell’attività” a un livello piuttosto alto.

ISO/IEC 27001

(“Information technology -- Security techniques -- Information security management systems – Requirements”)

è utilizzato per un percorso di certificazione

Standard

Cobit 5

Standard

Cobit 5

5 Perché
- Benefici
- Evitare Rischi
- Gestione ottimale Risorse

Interventi

3 Dove operare
- Processi
- Principi – Policies – Frameworks
- Sistemi
- Persone
- Organizzazione
- Informazioni disponibili
- Cultura / etica

Come operare
- Pratiche / Attività Base
  - Consolidate e universal-mente accettate
  - Riferimento ai principali Standard
  - Priorità in funzione obiettivi di business

4

2 Quando
- Governo
- Pianificazione Organizzazione
- Impostazione Definizione Soluzioni IT
- Erogazione Servizi Supporto
- Misura e Controllo

1 Attori
- CDA
- Business
- IT / IS
- Controllo

1. Chi
2. Quando
3. Dove
4. Come
5. Perché

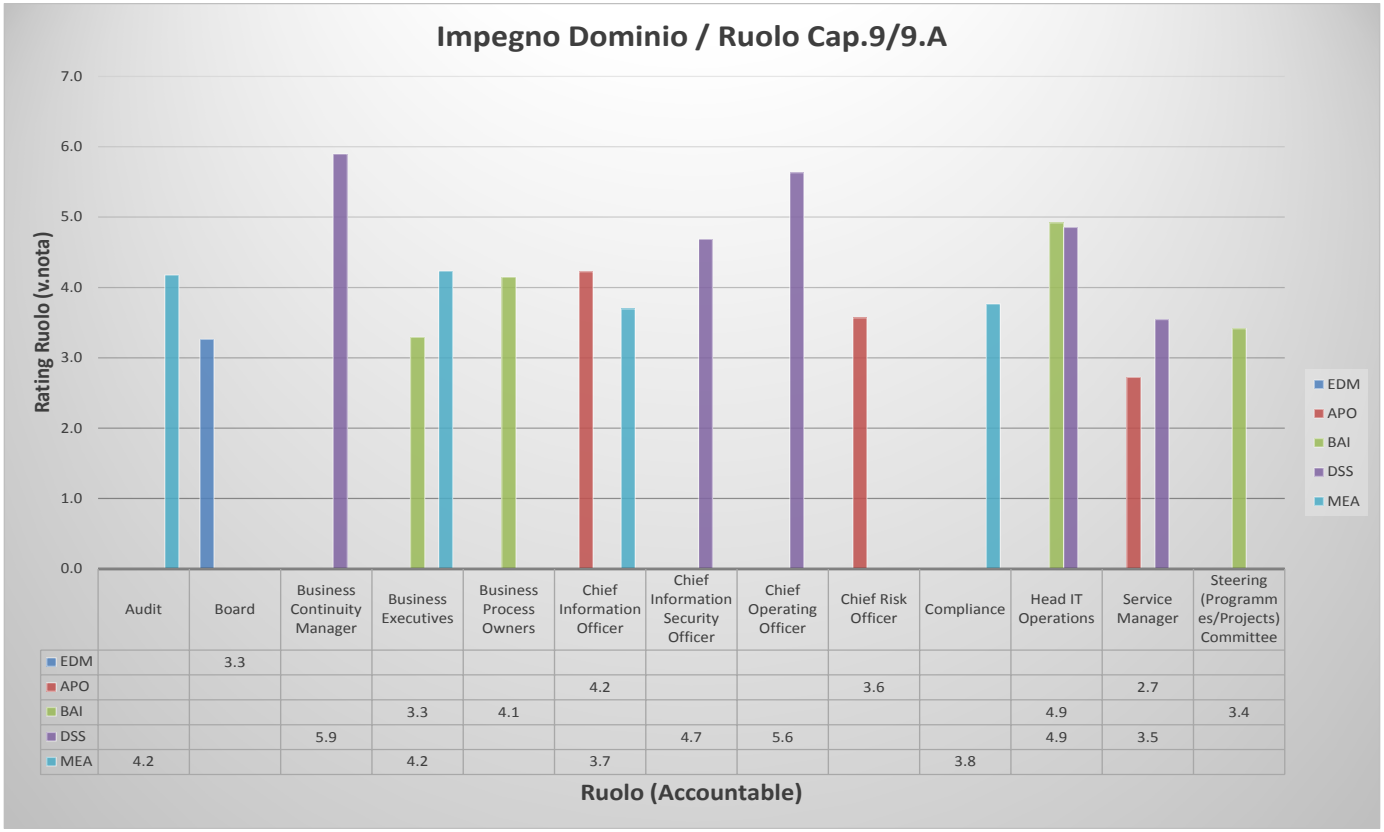
Gruppo di ricerca AIEA

Standard

Cobit 5

Indice	EDM05	APO01	APO07	APO09	APO12	BAI02	BAI04	BAI06	BAI07	BAI09	DSS01	DSS02	DSS04	MEA01	MEA02	MEA03	Tot
TITOLO V		**1.8**											**3.7**				**3.7**
Capitolo 9 - LA CONTINUITA' OPERATIVA		**1.8**											**3.7**				**3.7**
1. Destinatari		1.5											3.7				3.7
4. Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)		1.5											1.8				2.0
ALLEGATO A - REQUISITI PER LA CONTINUITÀ OPERATIVA	**2.3**		**2.2**	**1.9**	**2.9**	**2.3**	**3.5**	**3.0**	**1.5**	**2.7**	**3.3**	**2.9**	**4.3**	**2.9**	**2.8**	**3.1**	**4.5**
SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE													**3.6**				**3.6**
1. Premessa													3.6				3.6
SEZIONE II - REQUISITI PER TUTTI GLI OPERATORI				**1.9**	**2.5**	**2.3**	**3.4**	**3.0**	**1.5**	**2.6**	**3.2**		**3.9**	**2.7**	**2.2**	**2.9**	**4.2**
1. Ambito del piano di continuità operativa						2.1		2.9			3.2		2.9				3.5
2. Analisi di impatto					2.5		3.4			2.6							3.5
3. Definizione del piano di continuità operativa e gestione delle crisi				1.9		1.9		2.3	1.5				3.9	2.7	2.2	2.9	4.0
SEZIONE III - REQUISITI PARTICOLARI PER I PROCESSI A RILEVANZA SISTEMICA	**2.3**		**2.2**		**2.7**		**2.7**			**2.1**	**2.4**	**2.9**	**3.8**	**2.5**	**2.6**	**2.7**	**4.0**
1. Premessa													2.8			1.9	2.9
2. Definizione del piano di continuità operativa e gestione delle crisi			2.2		2.6		2.7			2.1	2.4	2.5	3.6	2.5	2.0	2.6	3.8
3. Comunicazioni alla Banca d'Italia	2.3				1.9							2.7	3.0		2.5		3.3
Tot	**2.3**	**1.8**	**2.2**	**1.9**	**2.9**	**2.3**	**3.5**	**3.0**	**1.5**	**2.7**	**3.3**	**2.9**	**4.4**	**2.9**	**2.8**	**3.1**	**4.5**

Cobit 5: chi è coinvolto e quando



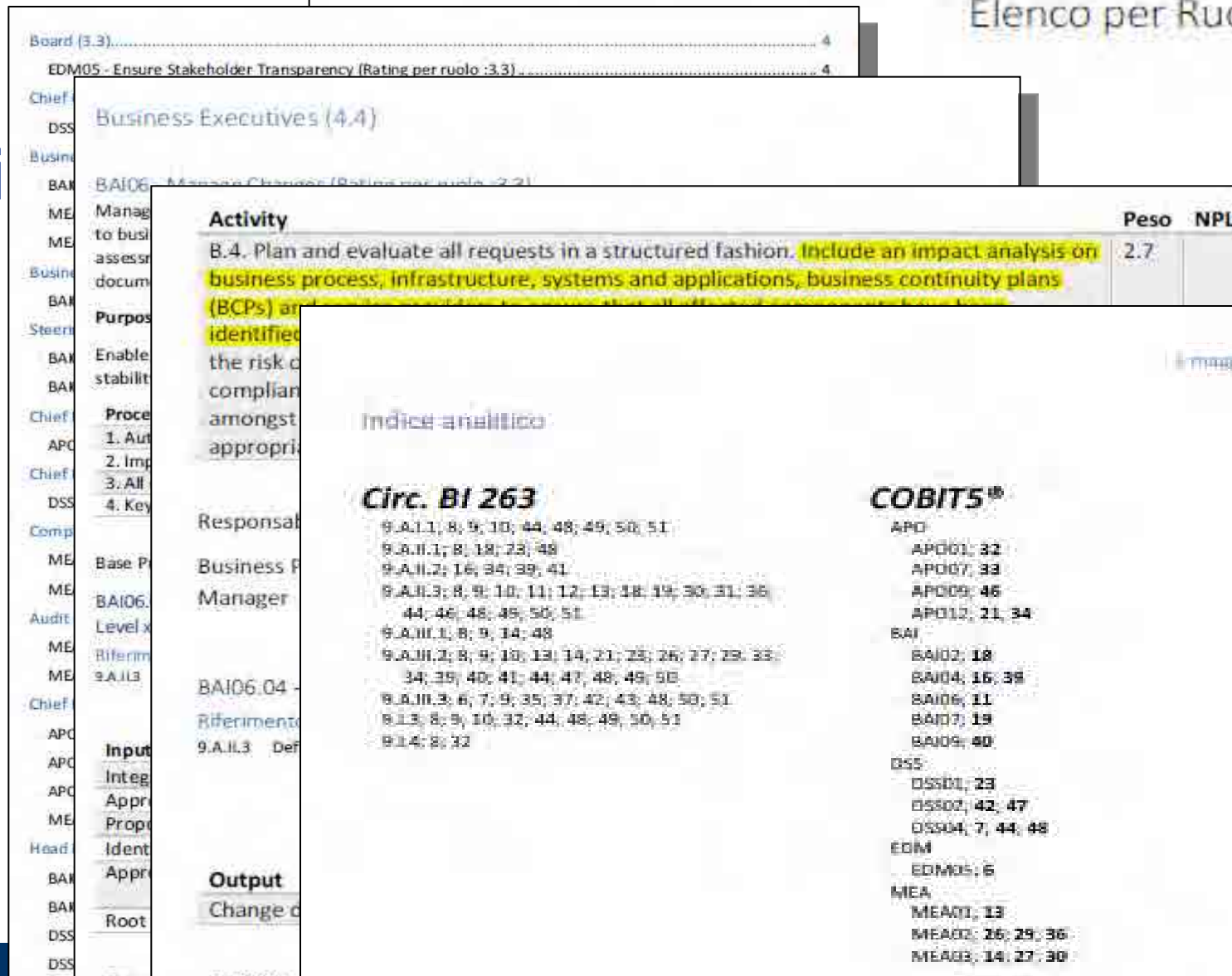
	Audit	Board	Business Continuity Manager	Business Executives	Business Process Owners	Chief Information Officer	Chief Information Security Officer	Chief Operating Officer	Chief Risk Officer	Compliance	Head IT Operations	Service Manager	Steering (Programmes/Projects) Committee
EDM		3.3											
APO						4.2			3.6			2.7	
BAI				3.3	4.1						4.9		3.4
DSS			5.9				4.7	5.6			4.9	3.5	
MEA	4.2			4.2		3.7				3.8			

Esempio

EDM APO BAI DSS MEA

Standard

Cobit 5 Ruoli e processi



Cobit 5: visione olistica

1. Processi
2. Informazioni (Inputs ed Outputs)
3. Organizzazione (RACI)
4. Principi e policies
5. Strumenti
6. Skills
7. Cultura ed Etica

Standard

ABISERVIZI ABI FORMAZIONE

INTERNATIONAL STANDARD

ISO 22301

First edition
2012-05-15

Societal security — Business continuity management systems — Requirements

Sécurité sociétale — Gestion de la continuité des affaires — Exigences

Standard

ISO 22301

ISO 22301:2012(E)

Contents

Page

Foreword iv

0 Introduction v
0.1 General v
0.2 The Plan-Do-Check-Act (PDCA) model v
0.3 Components of PDCA in this International Standard vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

Standard

ISO 22301

Capitolo 4 – "l'organizzazione" e lo scopo del BCMS

4.1 Understanding of the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose

La 22301, particolarmente nel capitolo 4 dedicato a "capire" l'azienda e determinare lo scopo del BCMS, sottolinea più volte l'importanza che il **BCMS** tenga debito conto e sia **correlato** con la **stategia** complessiva di **Risk Management** e con il **Risk Appettite Framework**

4 Context of the organization
4.1 Understanding of the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the business continuity management system
4.4 Business continuity management system

Standard

ISO 22301

Capitolo 5 – Leadership

Il **Top Management deve dimostrare e fornire evidenza** del suo **ruolo di guida** ed il suo **impegno** nel BCMS:

- ❑ Stabilendo la "policy", obiettivi, ruoli e responsabilità
- ❑ Motivando le persone a contribuire all'efficacia del BCMS
- ❑ Assicurando risorse necessarie (budget!!)
- ❑ Promuovendo il miglioramento continuo del BCMS
- ❑ Nominando il/i responsabili del BCMS, con le necessarie competenze

5 Leadership
5.1 Leadership and commitment
5.2 Management commitment
5.3 Policy
5.4 Organizational roles, responsibilities and authorities

Standard

ISO 22301

Capitolo 6 – Pianificazione

Pianificare le **azioni** per **indirizzare rischi ed opportunità**, **assicurando** che il sistema sia in grado di **raggiungere gli obiettivi** prefissati, che devono:

- Indicare il livello minimo di servizio accettabile
- Essere misurabili
- Essere monitorati e rivisti se necessario

6 Planning
6.1 Actions to address risks and opportunities
6.2 Business continuity objectives and plans to achieve them

Standard

ISO 22301

Capitolo 7 – Support

Prevedere siano predisposte **le risorse**, in tutti i sensi, necessarie per **disegnare, implementare, mantenere e migliorare continuamente il BCMS**:

- ✓ Competenze del personale, in particolare di chi opera nell'ambito della BC
- ✓ Awarness – Consapevolezza a tutti i livelli
- ✓ Comunicazione interna ed esterna e relative regole
- ✓ le regole per la creazione, modifica e gestione di tutta la documentazione, nei più opportuni formati per essere utilizzabile

7 Support
7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information

Standard

ISO 22301

Capitolo 8 – L'operatività

E' il capitolo più "operativo" in cui sono riportate le **indicazioni** su **come devono essere**:

- Stabiliti i **criteri**/parametri
- Eseguite la **BIA** ed il **risk assesment** (vedi anche risk appetite)
- Definita la **strategia** di BC
- Implementate le **procedure**, con particolare riguardo alla **rilevazione degli incidenti** ed alla **comunicazione**
- Strutturati, con indicazione dei **contenuti**, **i Piani**
- Eseguiti e documentati i **test**

8 Operation
8.1 Operational planning and control
8.2 Business impact analysis and risk assessment
8.3 Business continuity strategy
8.4 Establish and implement business contin ocedures
8.5 Exercising and testing

The organization shall ensure that outsourced processes are controlled.

Standard

ISO 22301

Capitolo 9 – Valutazione
9.2 – Internal Audit

Importante come un **intero capitolo** sia dedicato alla **valutazione del BCMS**. In particolare:

- **Perimetro, metodi e tempi** del monitoraggio e delle verifiche
- **Procedure documentate** di verifica
- **Pianificare, implementare e mantenere un programma di audit**
- **Coinvolgimento** del **top managemet**

9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management review

Standard

ISO 22301

Capitolo 10 – Miglioramento

Miglioramento continuo di **idoneità**, **adeguatezza** ed **efficacia** del BCMS.

A fronte di **non conformità** devono essere messe in atto le opportune **azioni correttive**, successivamente verificate

10 Improvement
10.1 Nonconformity and corrective action
10.2 Continual improvement

Programma corso: parte 1

Definizioni

Normativa

Standard

Possibili soluzioni

Alta affidabilità

Disaster recovery

Alta affidabilità (alta disponibilità)

- **Ridondanza:**
  - **Componenti dei server:**
    - Dischi
    - Alimentatori
    - Schede
  - **Server**
  - **Apparecchiature di rete**
  - **Dati**

Alta affidabilità (alta disponibilità)

Ridondanza impianti:

- Alimentazione
- Rete interna
- Connettività esterna

Misure di protezione:

- Antincendio
- Anti intrusione
- …

Alta affidabilità (alta disponibilità)

Elementi di criticità

– se un solo elemento non è ridondato crea un punto di debolezza significativo

Alta affidabilità (alta disponibilità)

E’ inutile che i sistemi centrali siano disponibili se non sono raggiungibili, ad esempio per:

- mancanza di rete
- mancanza del servizio

Oppure se nessuna della postazioni utente è disponibile ad esempio per:

- mancanza di alimentazione

Alta affidabilità (alta disponibilità)

Oppure se le postazioni non sono utilizzabili ad esempio per:

- Inagibilità temporanea dei locali
- Irraggiungibilità dei locali
- Mancanza dei servizi elementari (acqua, riscaldamento…)

Alta affidabilità (alta disponibilità)

Mettere sotto gruppo di continuità:

- Condizionatori
- Postazioni utente vitali
- Illuminazione essenziale

Attenzione al posizionamento delle batterie tampone

Contratto per rifornimento carburante anche durante week end

- Valvole dell'impianto di alimentazione di emergenza

Alta affidabilità (alta disponibilità)

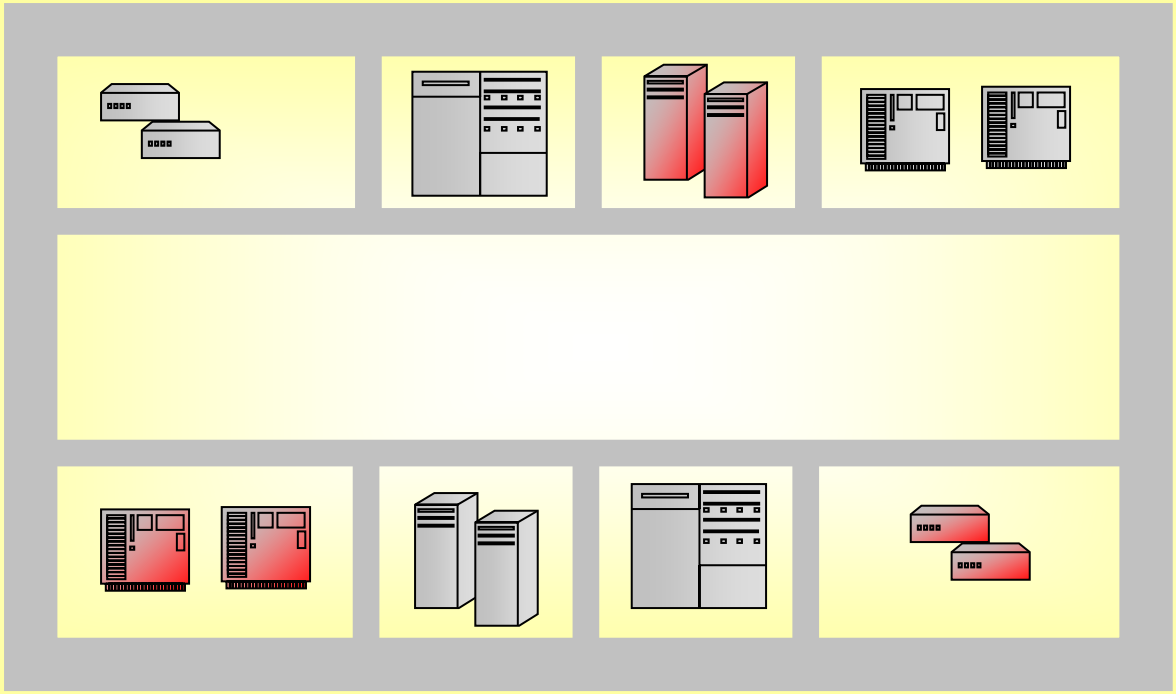
Possibilità di gestire in modalità remota il CED

Divieto di un solo operatore nel CED

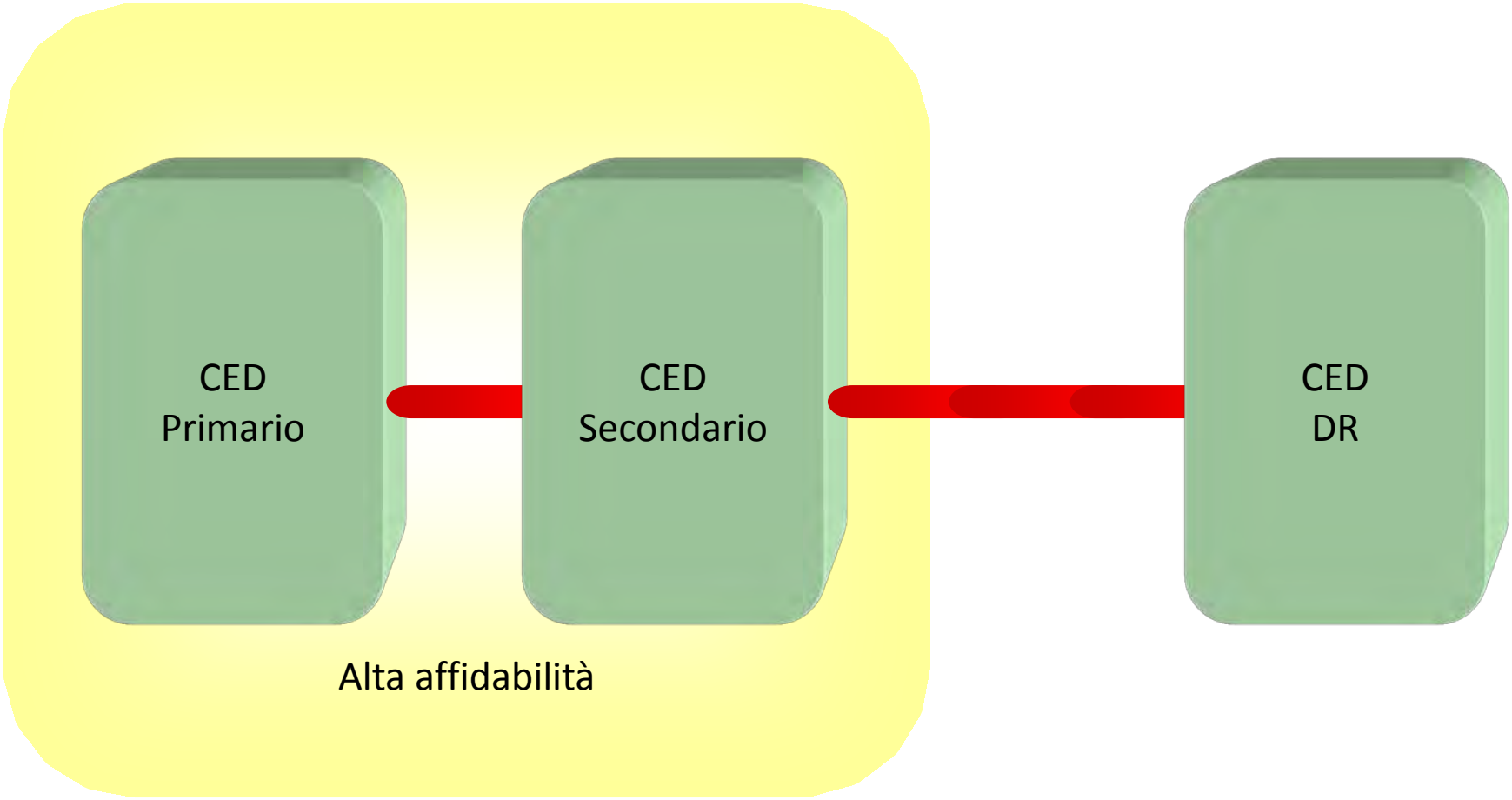
Possibilità di raggiungere da remoto il CED da parte degli utenti:

- VPN

Alta affidabilità: possibili soluzioni



Alta affidabilità: possibili soluzioni



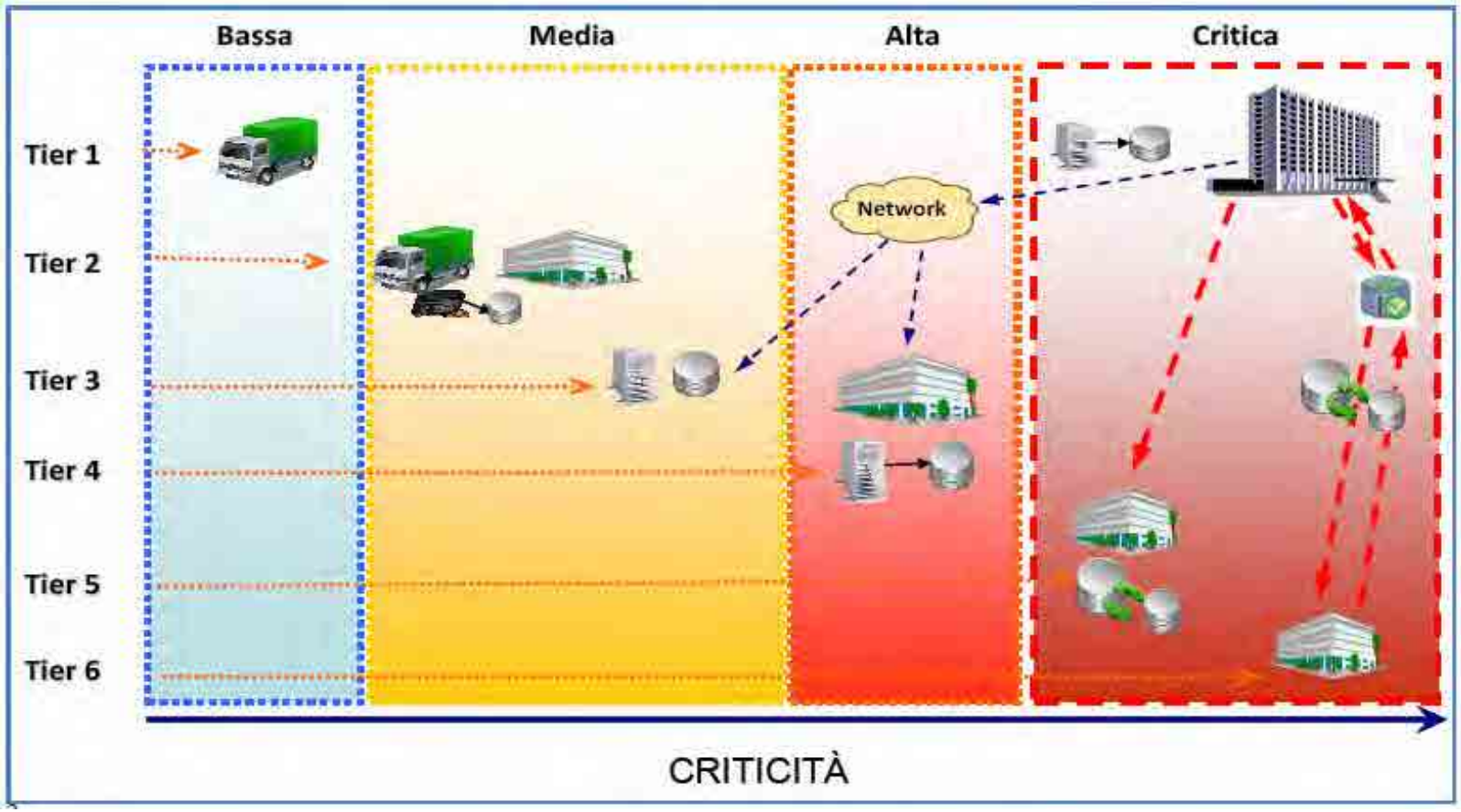
Disaster Recovery: possibili soluzioni

La creazione di soluzioni di DR comprende una casistica pressoché illimitata, in quanto molteplici sono le composizione dei sistemi informativi delle aziende di grosse dimensioni.

In estrema sintesi comunque è possibile distinguere le macro soluzioni di DR in alcune categorie:

- ❑ quelle che prevedono la disponibilità di un sito, nel quale è possibile collocare i sistemi su cui far ripartire applicazioni e servizi
- ❑ quelle che prevedono la disponibilità di un sito, con già disponibili i sistemi su cui far ripartire applicazioni e servizi, lasciati inattivi
- ❑ quelle che prevedono la disponibilità di un sito, nel quale sono disponili sistemi, già attivi che erogano applicazioni e servizi; in questo caso si utilizza normalmente un bilanciamento di carico fra i due siti (quello primario e quello secondario) nella erogazione dei servizi. In caso di fault di uno dei siti l'altro è in grado di erogare il 100% dei servizi, eventualmente con prestazioni degradate.

Disaster Recovery: possibili soluzioni



Disaster Recovery: possibili soluzioni

I LIVELLI DELLE SOLUZIONI *(Tier LG)*	PRINCIPALI INDICATORI			ELEMENTI DI MASSIMA DELLA SOLUZIONE TECNICA (SOLUZIONI ALMENO A 2 SITI)	
	RTO		RPO max	*Modalità minime di copia/aggiornamento per il conseguimento dei valori max di RPO*	*Aspetti minimali connessi al sito di DR*
	Min	Max			
Tier 1:	7g	>7 gg solari	max 7gg solari	Copia su supporti rimuovibili	Sito esistente ma da attrezzare con risorse elaborative/ server solo reperibili. Il sito di DR è predisposto ad accogliere personale e apparecchiature, ma rimane privo di risorse fino al momento di effettiva necessità. Di solito consiste solo di un ambiente fisico dotato di corrente elettrica e di rete dati con idonee misure di sicurezza (es: sistema antincendio ed antifumo; sistema antiallagamento; sistema di alimentazione in grado di garantire l'erogazione di energia elettrica anche a fronte di prolungate interruzioni di alimentazione nella cabina di fornitura; sistema d'aria condizionata per garantire temperatura ed umidità costante; impianto per il ricambio d'aria; sistema di accesso controllato).
Tier 2:	3g	max 7 gg	max 7 gg solari	Copia su supporti rimuovibili	Il sito dispone di hw e connettività già funzionante ma su scala inferiore rispetto al sito principale o a un sito alternativo sempre disponibile e con replica costante dei dati.
Tier 3:	1g	3g	Max 1 gg	Electonic vaulting: soluzione che comporta il backup dei dati presso il sito alternativo in maniera elettronica, con una riduzione del tempo necessario per il trasporto dei dati e la possibilità di un recovery time piu' veloce.	Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un site alternativo sempre disponibile e con replica costante dei dati. Il backup avviene in modalità elettronica e quindi sono necessari collegamenti fra i siti tenuto conto della tipologia, quantità e periodicità dei dati da backup-are

Tratto da "Linee Guida per il Disaster Recovery (DR) delle PA"

Disaster Recovery: possibili soluzioni

I LIVELLI DELLE SOLUZIONI *(Tier LG)*	PRINCIPALI INDICATORI			ELEMENTI DI MASSIMA DELLA SOLUZIONE TECNICA (SOLUZIONI ALMENO A 2 SITI)	
	RTO		RPO max	*Modalità minime di copia/aggiornamento per il conseguimento dei valori max di RPO*	*Aspetti minimali connessi al sito di DR*
	Min	Max			
Tier 4:	4h	3gg	Max 4 h	Asincrono On line (risorsa storage accesa)	Il sito alternative è solitamente "un duplicato" del sito originale con tutti i sistemi hardware e la quasi totalità dei backup di dati disponibile. Il sito alternativo può essere pronto ed operativo in alcune ore o meno. Nel caso in cui il personale deve essere spostato fisicamente presso il sito secondario, il sito risulterà operativo solo dal punto di vista del data processing. La piena operatività sarà raggiunta quando anche il personale avrà raggiunto il sito.
Tier 5:	1h	max 4 h	max 5 min	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi ciascuno con capacità sufficiente a prendere in carico il lavoro dell'altro e in cui l'aggiornamento del dato avviene solo quando entrambi i siti hanno completato l'update (con perdita dei soli i dati che in quel momento stanno per essere processati). E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.
Tier 6:	0m	1h	Zero min.	Aggiornamento Sincrono (risorsa storage accesa)	E' la soluzione che prevede due siti attivi, ognuno dei quali possiede capacità sufficienti a farsi carico del lavoro dell'altro; in questa soluzione il carico di lavoro da un sito all'altro si trasferisce immediatamente ed automaticamente. E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.

Tratto da "Linee Guida per il Disaster Recovery (DR) delle PA"

Disaster Recovery: criteri

R.1.01	Il sito dovrà avere un'opportuna distanza in linea d'aria dal sito primario, ove risiede il sistema Informativo dell'Amministrazione. Ove sia richiesta una soluzione con modalità di aggiornamento sincrono, allo stato attuale della tecnologia nell'individuare la distanza e la localizzazione del sito, non si può prescindere dalle caratteristiche della connettività sia in termini di distanza che di latenza, in quanto la "sincronizzazione", non è possibile al di sopra di certe distanze fisiche fra sito primario e secondario
R.1.02	Le aree adibite ad ospitare i sistemi di ripristino devono essere dislocate su di un unico sito
R.1.03	Il sito dovrà essere in regola con tutte le concessioni edilizie ed i permessi rilasciati dagli uffici competenti del Comune sul quale sorge lo stesso.
R.1.04	Qualora il sito di DR sia costruito su territorio soggetto ad attività sismica, lo stesso deve avere una struttura progettata per minimizzare gli impatti dell'onda sismica, attraverso la riduzione del numero di piani, il consolidamento dei piani inferiori e l'utilizzo di materiali di alta qualità, che possano resistere alle vibrazioni provocate dal sisma e che prendano fuoco difficilmente. Pertanto, si richiede l'attestato di valutazione di rischio sismico coerente con la l'area geografica che ospita il sito.
R.1.05	Il sito di DR non deve essere localizzato in una regione affetta da tempeste di ghiaccio e neve.
R.1.06	Il sito di DR non deve essere localizzato in aree soggette ad allagamenti e/o alluvioni.
R.1.07	Il sito di DR non deve essere localizzato in aree soggette a frane.
R.1.08	Il sito di DR non deve essere localizzato vicino ad aeroporti, centrali elettriche o stazioni di scambio ferroviario per evitare il fenomeno di interferenza da emissioni elettromagnetiche
R.1.09	Il sito di DR deve avere un impianto con luci di emergenza, completo di linee di distribuzione ed opportunamente sezionato con interruttori magnetotermici differenziali al quadro elettrico, deve avere una configurazione composta da corpi illuminanti stagni IP 44 in materiale termoestinguente, con led di segnalazione di presenza di rete, cablate con lampade da 18 W, con batterie tampone in grado di garantire un minimo di 3 ore di funzionamento in caso di mancanza di tensione.
R.1.10	Il sito di DR deve avere un impianto di illuminazione primaria completo di linee di distribuzione, interruttori ed opportunamente sezionato con interruttori magnetotermici differenziali al quadro elettrico, in grado di garantire su tutta la superficie utile del sito un illuminamento a "tutto acceso" pari a 600 Lux.

Tratto da "Linee Guida per il Disaster Recovery (DR) delle PA"

Disaster Recovery: criteri

R.2.01	Il pavimento antistatico soprelevato dovrà avere una altezza utile non inferiore a cm 25 con supporto di carico distribuito superiore a 2.500 Kg/mq e carico di punta pari o superiore a 500 Kg.
R.2.02	La soletta dovrà essere in grado di supportare carichi di almeno 500 Kg/mq, evidenziata da relativa certificazione di collaudo rilasciata da ente o professionista abilitato. Le solette dovranno essere opportunamente sigillate al fine di garantire l'adeguata resistenza al fuoco e prevenire la circolazione di polvere.
R.2.03	Il pavimento flottante dovrà avere una struttura modulare con modulo 60 cm x 60 cm, resistenza al fuoco minima pari a REI 60 e spessore minimo pari a circa 4 cm.
R.2.04	L'altezza utile dal pavimento flottante dovrà essere di almeno 270 cm.
R.2.05	Presenza di sensore installato sulla pavimentazione esistente sotto il pavimento flottante, in grado di rilevare il liquido ad una altezza variabile tra 0 ed 11 millimetri. Tale dispositivo dovrà avere funzioni di test e di inibizione da remoto, oltre alla possibilità di regolazione della soglia di allarme. Grado di protezione IP 67.
R.2.06	Presenza di punti manuali di attivazione degli allarmi dotati di dispositivo di isolamento dai cortocircuiti sulla linea di rilevazione, attivabili mediante azione su lastra di vetro con punto di rottura e azionamento pulsante.
R.2.07	Presenza di segnalatori acustici installati, in concomitanza a segnalatori luminosi di allarme, con potenza sonora di 95 dB, indicanti almeno le seguenti condizioni: "ALLARME INCENDIO", "SPEGNIMENTO IN CORSO", "ALLARME EVACUAZIONE", "ALLARME ALLAGAMENTO".

Tratto da "Linee Guida per il Disaster Recovery (DR) delle PA"

Disaster Recovery: criteri

R.3.01	L'alimentazione elettrica dell'infrastruttura ICT destinata a ripristinare i sistemi dovrà essere garantita da sistemi ridondati ed in parallelo costituiti da gruppi elettrogeni e sistemi UPS a garanzia dell'erogazione con continuità e qualità dell'alimentazione elettrica (continuità di erogazione e qualità della tensione) a fronte di guasti e/o distacchi (programmati o no) a carico della rete di distribuzione.
R.3.02	Presenza di almeno 2 gruppi di continuità (UPS) in configurazione parallela ridondata ed aventi batterie con autonomia di almeno 10 minuti a pieno carico e comunque congruo per l'attivazione del sistema di emergenza. Gli UPS dovranno assicurare la continuità a tutti i dispositivi informatici e l'illuminazione d'emergenza. I locali UPS e Batterie devono essere adeguatamente compartimentati con canalina di contenimento di eventuali fuoriuscite di liquidi, da sistema di condizionamento e, nel caso di batterie elettrolitiche, da sistema di espulsione gas e da rilevatori idrogeno.
R.3.03	Il sito deve essere in grado di operare in assenza di utilities esterne (acqua, gas, luce, etc.) per un periodo di tempo pari a 48 ore senza rifornimenti.
R.3.04	Nel caso di interruzioni superiori alle 48 ore deve essere previsto un piano di approvvigionamento alternativo, da quello della rete di distribuzione usuale, con fornitori terzi; in particolare per il carburante destinato ai gruppi elettrogeni.
R.3.05	Presenza di una doppia sorgente di alimentazione elettrica per i rack e/o i server installati. Le due linee di alimentazione devono essere mantenute entrambe attive anche durante gli interventi di manutenzione programmata mediante apposite operazioni di switch. Si richiede inoltre la presenza di static switch automatici in grado di ovviare ad una caduta su una delle due linee di alimentazione con trasferimento automatico del carico sulla seconda linea. Questi switch dovranno essere posizionati a livello dei quadri di piano o di sala.
R.3.06	Per quanto attiene le aree IT e TLC la distribuzione dovrà essere realizzata con doppio circuito di blindo-sbarre o cavi elettrici, a seconda del livello di distribuzione con diversi livelli di selettività al fine di evitare la propagazione del corto circuito, alimentate/i da quadri elettrici separati. Relativamente all'area TLC, si richiede la presenza di una adeguata infrastruttura di telecomunicazione destinata ad ospitare gli apparati necessari per i collegamenti WAN e a garantire l'attestazione dei collegamenti SPC.

Tratto da "Linee Guida per il Disaster Recovery (DR) delle PA"

Disaster Recovery: criteri

R.3.07	Presenza di switch dell'alimentazione dei condizionatori di sala per consentire il passaggio automatico alla seconda linea di alimentazione in caso di caduta sulla prima. Le caratteristiche richieste sono le seguenti: o tensione di alimentazione a 400 Volt 3F e 240 Volt MF; o potenza media minima erogabile 0,5 KVA/mq (solo carico IT) con possibilità di incremento a 0,8 KVA/mq; o utenze sezionabili con interruttori automatici magnetotermici e con salvavita; o anello di terra unico (equipotenzialità). Pulsante di sgancio manuale (Emergency Power Off) dove necessario.
R.3.08	Presenza di impianto di condizionamento del sito di DR ridondato con sensori per il controllo della temperatura e dell'umidità.
R.3.09	Sistema di monitoraggio continuo della temperatura nell'area del datacenter attraverso sensori per la segnalazione dell'allarme connesso al superamento delle temperature ammesse per il corretto funzionamento delle macchine all'interno del datacenter.
R.3.10	Presenza di impianto di condizionamento adeguato a garantire la piena operatività degli apparati di ripristino anche in caso di guasto alle singole componenti dell'impianto (sia relativamente alla distribuzione che relativamente alle unità di condizionamento).
R.3.11	Sistema di rilevazione anti incendio costituito da rilevatori di fumi e calore in grado da allarmare il personale di sorveglianza e attivare automaticamente gli impianti di spegnimento.
R.3.12	Presenza di impianto di rilevazione fumi progettato nel pieno rispetto della normativa UNI 9795 con garanzia della segmentazione dello stesso e la conseguente perdita delle sole zone oggetto di eventuale manutenzione, incidente o calamità naturale, ma con il continuo funzionamento del resto dell'impianto.
R.3.13	Sistema di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso di tipo ARGON o altri gas non alogenati. L'impianto deve permettere di controllare più focolai contemporanei, evitando invasioni di fumo, sbalzi improvvisi di temperatura e dispersione di residui nocivi per l'uomo e per le apparecchiature. L'efficacia delle bombole o serbatoi dell'estinguente dovrà essere verificata in accordo con le norme vigenti. La collocazione delle bombole dovrà essere in locale separato dell'edificio.
R.3.14	Previsione di un adeguato sistema di bonifica dei locali "a scarica di gas avvenuta" per permettere il riutilizzo dei locali in breve tempo.
R.3.15	Monitoraggio 24hX7 degli impianti.

Tratto da "Linee Guida per il Disaster Recovery (DR) delle PA"

Disaster Recovery: criteri

ABISERVIZI ABI FORMAZIONE

Requisiti per la sicurezza del sito

R.4.01	I locali adibiti ad ospitare le infrastrutture di ripristino devono essere conformi a quanto previsto dalle attuali norme sulla sicurezza e salute sul luogo di lavoro dei lavoratori, di cui al DLgs.. n. 81/2008 e s.m.i.
R.4.02	Predisposizione di aree sicure dotate di appropriate barriere di sicurezza controllate tramite apposito sistema di videosorveglianza.
R.4.03	Accesso al sito regolato e controllato da procedure di riconoscimento e registrazione effettuato presso la reception.
R.4.04	Monitoraggio dell'ingresso principale attraverso telecamere a circuito chiuso con registrazione continua o attivabile attraverso sensore di movimento anche IR.
R.4.05	Protezione interna tramite sistema di telecamere a circuito chiuso.
R.4.06	Accesso alle sale macchine mediante identificazione/autenticazione attraverso un controllo elettronico e/o riconoscimento biometrico.
R.4.07	Sistema antintrusione che consenta di rilevare la presenza di persone all'interno delle aree sensibili.
R.4.08	Protezione esterna tramite sistema antiscavalcamento con illuminazione perimetrale, sistema di rilevamento presenza e telecamere a circuito chiuso controllate dal personale di sicurezza 24 ore su 24.

Requisiti per la Sicurezza interna e l'accesso all'edificio del sito

R.5.01	Identificazione di uno o più responsabile/i delle aree del sito per le autorizzazioni necessarie all'accesso.
R.5.02	Procedura di accesso alle aree per limitare l'accesso alle persone autorizzate dal responsabile, con almeno le seguenti classi di accesso: o personale del prestatore, o personale clienti del prestatore, o personale delegato dal prestatore (ad esempio personale che esegue manutenzione/riparazione, ecc.). La procedura deve anche regolare la gestione di badge/passi temporanei e le modalità di accompagnamento di personale esterno (clienti, manutenzione, ecc.) alle varie aree del sito da parte di personale del prestatore.

Altre caratteristiche

R.6.01	Presenza di aree ristoro nei piani che ospitano le postazioni di lavoro
R.6.02	Disponibilità di locale di pronto soccorso.
R.6.03	Conformità alle disposizioni in merito alla organizzazione del pronto soccorso aziendale, alla formazione degli addetti al pronto soccorso ed alle attrezzature necessarie per effettuare gli interventi di primo soccorso e gestione dell'emergenza sanitaria.

Tratto da "Linee Guida per il Disaster Recovery (DR) delle PA"

Disaster Recovery: problemi

La possibilità di realizzare un efficace ed efficiente piano di DR è che i sistemi siano progettati fin da subito a tale fine

Ovvero che il sistema sia particolarmente semplice o monolitico

Disaster Recovery: problemi

- Difficoltà nella scomposizione dei servizi/processi
- Mappatura delle risorse
- Difficile individuare le risorse necessarie
- Ci sono le infrastrutture comuni che non possono essere scomposte
- Corretta individuazione dei collegamenti interni ed esterni

Disaster Recovery: problemi

- Se i sistemi sono troppi la priorità di ripartenza comporta notevoli problemi
- Difficoltà nel ripristino legata alla mancata sincronizzazione dei dati
- Solo sistemi molto piccoli e limitati possono ripartire senza problemi, ovvero solo se si dispone effettivamente di un sito alternativo

Disaster Recovery: problemi

- Solo con i test è possibile verificare se funzionano effettivamente le soluzioni
- I test sono costosi, difficili, pericolosi
- Il rientro non è un opzione prevedibile; se si va in DR è perché il centro principale potrebbe non esserci più
- Necessità di una verifica da parte dell'audit

Disaster Recovery: problemi

- Per far si che una soluzione di DR funzioni non è sufficiente curare l'aspetto tecnico
- E' indispensabile definire il Piano di DR:
  - responsabilità
  - RTO, RPO (rispetto a cosa???)
  - procedura di dichiarazione di disastro
  - procedure di ripartenza
- Definizione di un glossario comune fra tutti gli attori coinvolti

Programma corso: parte 2

Piano di business continuity

- BIA
- Ruoli
- Fornitori/Outsourcer
- Verifiche

Piano di business continuity: perimetro

Banche del Gruppo (anche estere)

Società del gruppo che svolgono processi critici

Verifica che tutti i soggetti interessati siano ricompresi nell'attività di analisi svolta dal BCM

Piano di business continuity: ambito

incidenti di portata:

- settoriale
- aziendale

catastrofi estese che colpiscono l'operatore o le sue controparti rilevanti (altre società del gruppo; principali fornitori; clientela primaria; specifici mercati finanziari; sistemi di regolamento, compensazione e garanzia)

Piano di business continuity: scenari

Il piano di continuità operativa prende in considerazione diversi scenari di crisi basati almeno sui seguenti fattori di rischio, conseguenti a eventi naturali o attività umana, inclusi danneggiamenti gravi da parte di dipendenti:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
- indisponibilità di sistemi informativi critici;
- indisponibilità di personale essenziale per il funzionamento dei processi aziendali;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
- alterazione o perdita di dati e documenti critici.

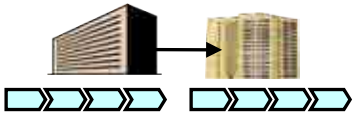
Piano di business continuity: scenari

ipotesi di **crisi estesa** e **blocchi prolungati delle infrastrutture essenziali**

tiene conto delle **vulnerabilità esistenti** e delle **misure preventive** poste in essere per garantire il raggiungimento degli obiettivi aziendali.

Business continuity: possibili soluzioni nei vari scenari

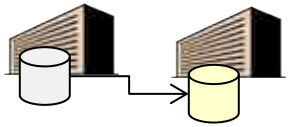
Distruzione o inaccessibilità di strutture nelle quali sono allocate:
- **unità operative**
- **apparecchiature critiche**



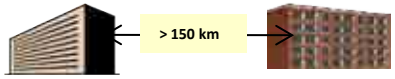
Backup reciproco per processi già svolti in più siti

Spostamento risorse critiche in sito equivalente (sistemi, infrastrutture, ecc.)

Spostamento risorse critiche in sito diverso preventivamente adeguato (sistemi, logistica, attrezzature, ecc..)



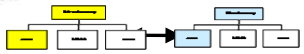
Ridirezione sul la copia sincrona dei dati



Attivazione della soluzione di Disaster Recovery

Indisponibilità di personale essenziale per il funzionamento dell'azienda

Processo già svolto in più siti: backup reciproco



Attivazione dell'Unità Organizzativa di backup

Interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari)

in dipendenza dell'infrastruttura in crisi

Attivazione generatori

Ridirezione fisso-mobile

altro … … …

nei casi più gravi, anche lo spostamento di risorse in siti equivalenti o attivazione di backup reciproci

tutte le soluzioni sono documentate

Piano di business continuity

Caratteristiche

- Completezza
- Facilità di fruibilità
- Disponibilità ed accessibilità in caso di crisi

Piano di business continuity

Piani gestiti direttamente dal BCM

Verifica

Piani acquisiti

Verifica di completezza e coerenza

Controparti rilevanti (fra cui Fornitori di processi /servizi/ infrastrutture)

Verifica contenuto

Piano di business continuity

Formalizzazione del piano

- Responsabilità di esecuzione
- Processo di emissione
- Processo di manutenzione periodica
- Processo di manutenzione nel continuo

Piano di business continuity

Alert in caso di modifiche a:

processi
sistemi
edifici
persone

Strumenti di gestione

Interfacciamento con fonti dati

Piano di BC: gestione della crisi

la procedura per la dichiarazione dello stato di crisi è definita in raccordo con il processo di gestione degli incidenti di sicurezza informatica e delle altre tipologie di incidenti;

- sicurezza informatica
- personale
- edifici
- utilities
- Infrastrutture

Piano di BC: gestione della crisi

Dichiarazione dello stato di crisi:

- ❑ presupposti
- ❑ modalità
- ❑ autorità preposta a farlo
- ❑ misure di escalation rapide per la dichiarazione dello stato di crisi

Piano di BC: gestione della crisi

Struttura che gestisce lo stato di crisi

- membri che la compongono
- Capo

- ✓ modalità di comunicazioni interne
- ✓ responsabilità attribuite alle funzioni aziendali interessate
- ✓ catena di comando che gestisce l'azienda in caso di crisi

Piano di BC: rientro dall'emergenza

Il piano di continuità operativa indica:

- ❑ le procedure per il rientro dall'emergenza
- ❑ la rilevazione dei danni
- ❑ la gestione di tutte le operazioni di rientro
- ❑ la verifica dell'operatività per i servizi ripristinati.
- ❑ iter per riprendere la normale operatività

Piano di BC: comunicazione

Il piano di continuità operativa definisce le modalità di comunicazione con la clientela, le controparti rilevanti, le autorità e i media.

Piano di BC: comunicaz. a Banca d'Italia

In caso di situazione di crisi che non assumano rilevanza sistemica per il sistema finanziario, le banche e i gruppi bancari contattano, al fine di agevolare il coordinamento degli interventi, la Banca d'Italia.

In caso di crisi, successivamente al ripristino dei processi critici, l'operatore fornisce alla Banca d'Italia valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti

Piano di BC: problemi

- mancanza di documentazione
- assenza di una mappatura e formalizzazione dei processi
- parti di processi chiave non documentata o non nota
- ampio uso di applicazioni di operatività individuale in aggiunta al sistema informativo aziendale

Piano di BC: problemi

- dispersione nella archiviazione dei file, molto spesso collocati anche sui singoli pc in uso ai dipendenti
- assenza di un censimento della documentazione presente al di fuori del sistema informativo
- mancanza di qualunque classificazione delle informazioni
- eccessivo ricorso a figure chiave
- mancanza di backup per quanto attiene la documentazione

Piano di BC: Piano di DR

Misure di prevenzione

- ✓ descrizione dei sistemi di alta affidabilita’

Piano di BC: Piano di DR

- Modalità e frequenza di generazione delle copie
- Procedure per il ripristino presso i siti alternativi
- Frequenza delle copie degli archivi dei processi critici non può essere maggiore di 1 giorno
- Trasporto e conservazione in luoghi remoti ad elevata sicurezza fisica

Piano di BC: Piani operativi

Le procedure di continuità operativa sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non impegnate nell'ordinaria attività nei processi cui si riferiscono.

La documentazione della Business Continuity

La **gestione della Business Continuity** e del **BCMS richiedono** la predisposizione di **opportuna documentazione**, che deve essere **tenuta** tempo per tempo **aggiornata**.

La **tipologia** e le **modalità di gestione** sono fortemente **influenzati** dal **destinatario**, inteso come il fruitore di quanto documentato, e dalla **finalità** del documento.

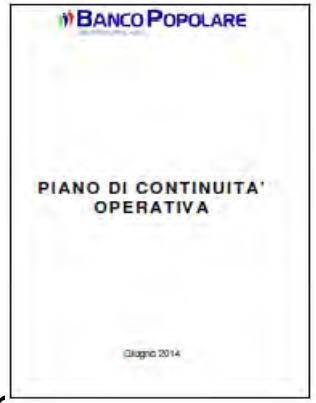
Appare infatti evidente la differenza che vi sarà, ad esempio, tra il "Piano di Continuità Operativa" destinato all'approvazione del Consiglio di Amministrazione e la documentazione tecnica necessaria al riavvio di un server in caso di necessità.

Nelle slides successive è riportata una esemplificazione di strutturazione della documentazione.
E' fondamentale, indipendentemente dalle modalità adottate, che emerga da quanto documentato la completa copertura dell'intero perimetro del BCMS.

La documentazione della Business Continuity

Il **Piano di Continuità Operativa** è generalmente un **documento** in formato **cartaceo** che riporta:

- ⇨ Le **policy** della Banca in tema di Business Continuity
- ⇨ Le **linee guida** seguite nella realizzazione del **BCMS**
- ⇨ Le modalità di **gestione del BCMS**
- ⇨ Gli **obiettivi di continuità** stabiliti
- ⇨ I **processi** che rientrano **nel perimetro** della Business Continuity
- ⇨ Le **strategie** adottate per fare fronte ad eventi di **crisi**
- ⇨ Le **modalità** di **rilevazione** degli **incidenti** e l'**attivazione** della **crisi**
- ⇨ Gli **organi di governo** della crisi e della Banca in caso di crisi



Il documento, che non entra in dettagli operativi, è **approvato dal Consiglio di Amministrazione** ed indica chiaramente la presenza di allegati operativi che ne formano parte integrante e che vengono mantenuti costantemente aggiornati.

Può essere utile inviare al Consiglio la versione degli allegati disponibile alla data di approvazione del Piano.

La documentazione della Business Continuity

Vengono poi generalmente prodotti **uno o più "Allegati operativi"** che, a seconda della struttura della Banca e delle sue dimensioni, possono essere **strutturati**:

- Per processo
- Per edificio
- Per scenario di rischio
- …

Questi documenti, non necessariamente cartacei, devono essere **facilmente manutenibili** per essere **costantemente aggiornati con le modifiche organizzative**, meglio se gestiti da apposita procedura informatica, e contengono:

- La **descrizione delle attività** che devono essere messe in atto
- Gli **strumenti**, applicazioni-procedure-supporti, che devono essere utilizzati
- Il **"chi fa cosa"** fondamentale per evitare perdite di tempo e sovrapposizioni
- L'elenco dei **contatti** con le relative **call tree** (numeri di telefono ed indirizzi email)

La documentazione della Business Continuity

Devono inoltre essere predisposti, e rientrano a tutti gli effetti nella documentazione del BCMS, i **“Manuali operativi”** che:

➲ Vengono **redatti dai process owner** per essere utilizzati dalle risorse che svolgeranno le attività in caso di crisi

➲ Contengono le **attività di dettaglio** che devono essere svolte, con la spiegazione di come effettuarle, riportando, ad esempio, le **videate delle procedure** ed i valori da inserire in campi specifici

➲ Riportano i **riferimenti di controparti** operative che devono essere contattate in caso di necessità

E’ fondamentale che questi manuali vengano **verificati più volte nel corso dell’anno**, durante attività di formazione e/o di test, per garantire il loro allineamento con l’evoluzione operativa.

La documentazione della Business Continuity

Per potere verificare come sia stata correttamente svolta la Business Impact Analisys è necessario che sia sempre presente la **documentazione della BIA effettuata**, e dei relativi aggiornamenti.
Anche in questo caso le **modalità di redazione** delle evidenze può essere **varia**, ma devono essere **necessariamente presenti**:

☞ **Criteri di analisi** dei processi in relazione ai rischi potenziali

☞ **Punti di verifica** dell'attività svolta, come verbali delle riunioni effettuate con process owner, verifiche di regolamenti e/o normative aziendali

☞ Dettaglio dei **processi/attività analizzati** con la **valutazione** assegnata in termini di rischio in relazione ai criteri adottati

☞ **Strumenti**, applicazioni informatiche, telefoni registrati, documenti particolari, la cui disponibilità sia **necessari**a nell'erogazione del processo/attività

La documentazione può essere **strutturata per Processo**, per **Unità Organizzativa** o secondo altri parametri che comunque garantiscano la copertura di tutto il perimetro di operatività della Banca.

Un utile punto di riferimento è la **metodologia** predisposta da **ABILAB**.

La documentazione della Business Continuity

Come noto è da considerare un allegato al Piano di Continuità Operativa il **Piano di Disaster Recovery del sistema informativo**.
A sua volta il **Piano di DR**, sia considerato come un allegato sia che rappresenti un "Piano Settoriale", può essere, ed è consigliabile che sia**, articolato in più documenti**.

Un documento di **livello alto "Piano di Disaster Recovery,"** che, in analogia al Piano di BC, riporta le **linee guida, gli obiettivi di ripristino e le strategie di recovery** adottate redatto con un **linguaggio non troppo tecnico** per potere essere compreso anche dal top management senza skill specifici

La **descrizione dell'ambiente di produzione** e della relativa "**alta affidabilità**", da cui si possa evincere come il ricorso alle misure previste dal DR sia necessario solo in caso di eventi particolarmente avversi

La descrizione del **processo di Disaster Recovery**, con l'indicazione delle risorse coinvolte (con il relativo elenco dei contati), delle priorità, delle attività da svolgere

I **dettagli tecnici di riattivazione** dei singoli apparati, con precise indicazioni rivolte al personale incaricato e dotato delle opportune capacità operative

La documentazione della Business Continuity

Sono importanti i **documenti** che evidenziano l'**adeguatezza** del Piano di Continuità Operativa.

Verrà quindi **annualmente** redatto un **documento**, destinato al **Consiglio di Amministrazione** (ed al Collegio Sindacale), che **riassume le prove** effettuate sia **organizzative** sia **tecnoligiche**, evidenziando per ognuna di esse:

- **Obiettivi**
- **Modalità**
- **Risultati**
- **Eventuali problemi** e, nel caso, le **azioni correttive avviate** (e come si sono concluse)

Naturalmente devono anche essere predisposti **documenti di dettaglio** (verbale del test) che riportino in modo analitico:

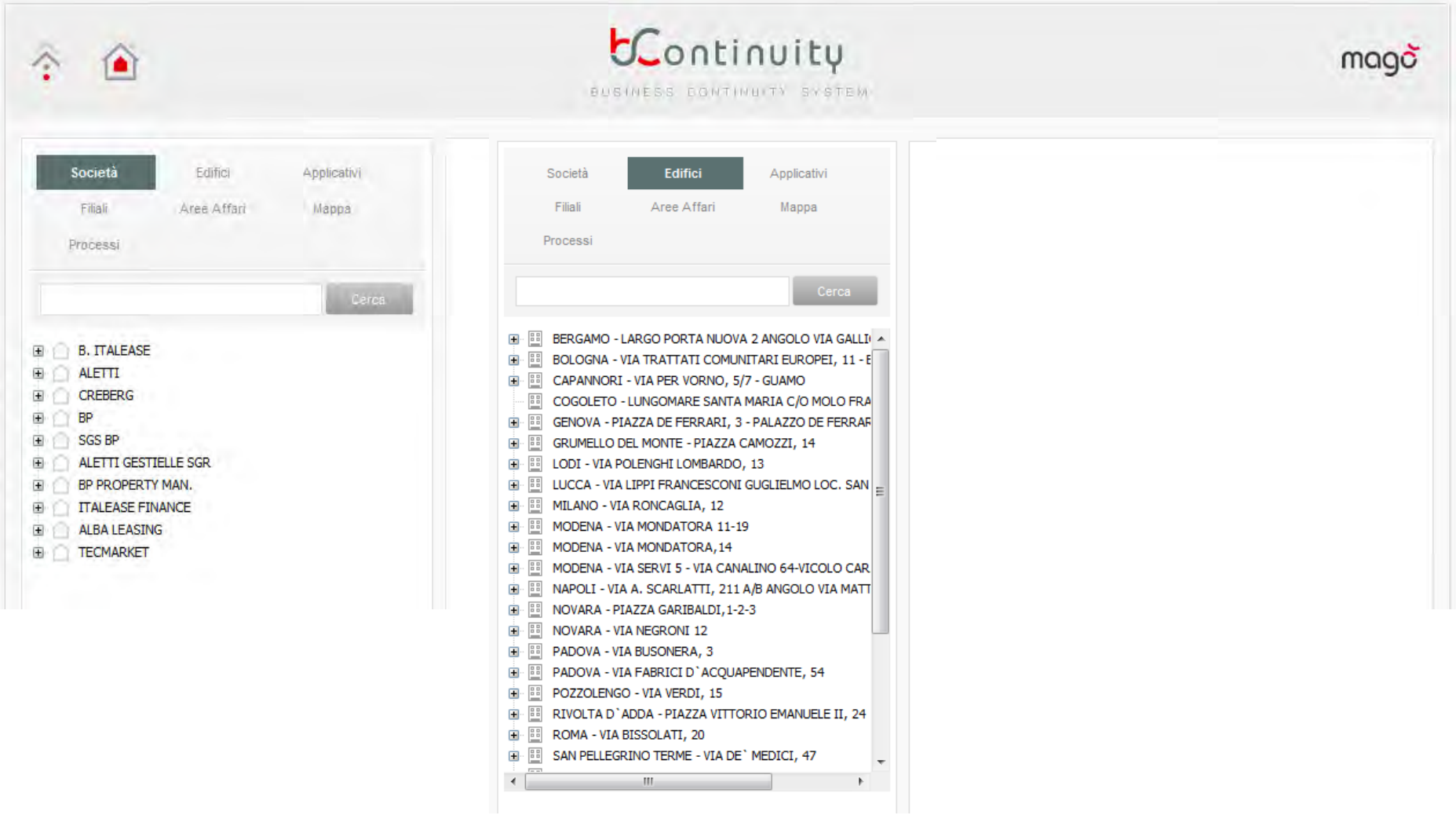
- **Scenario** ipotizzato
- **Date ed orari** di effettuazione
- **Risorse**, umane e tecnologiche, **coinvolte**
- **Operatività** svolta
- **Dettaglio** degli eventuali **problemi** riscontrati, eventualmente con il work around adottato
- **Azioni correttive** impostate

Strumento di Gestione

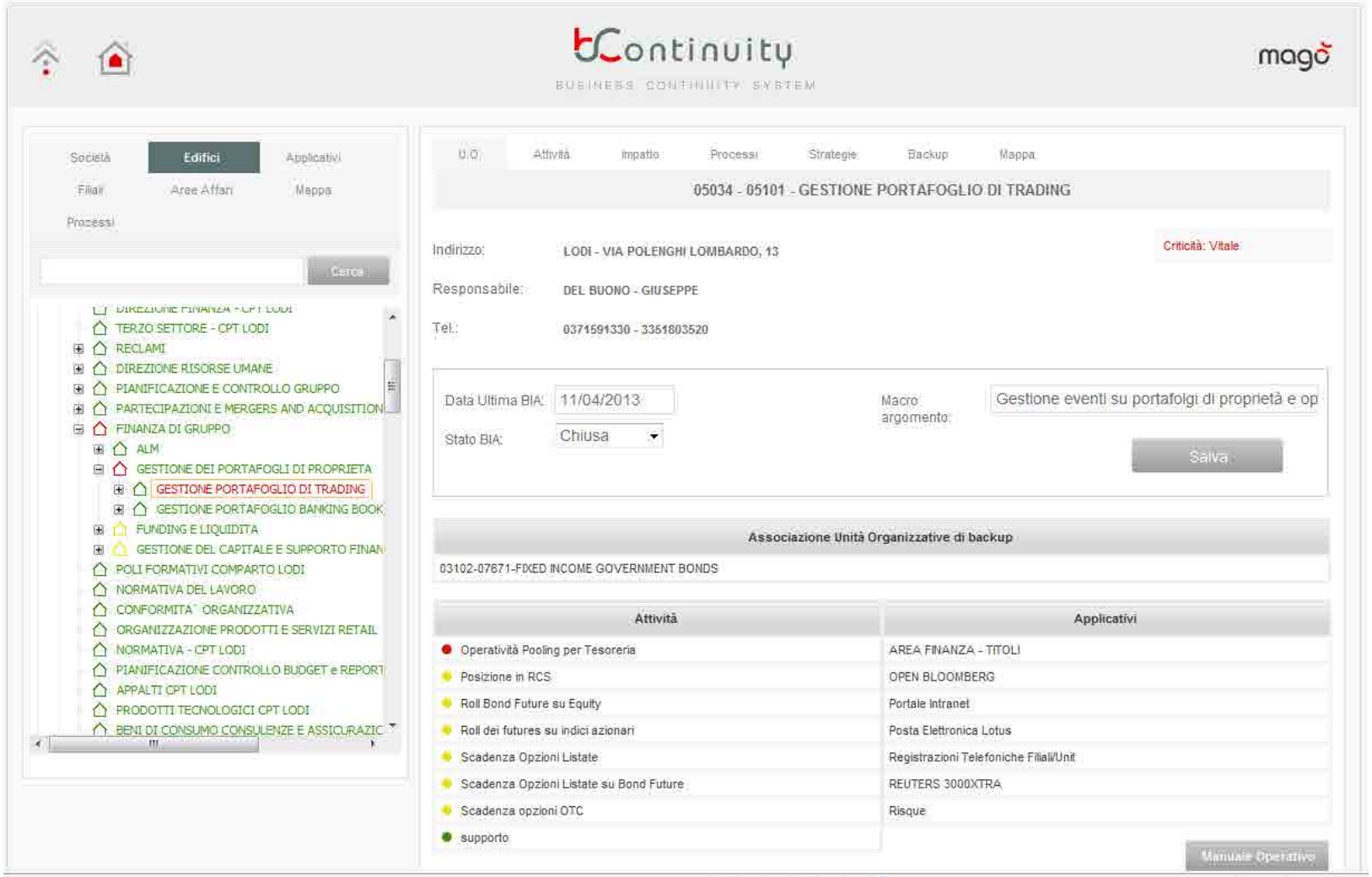
Strumento di Gestione

Matricola	Abi	Codice	Ruolo	Cognome	Nome	Telefono Banca	Telefono Privato	Cellulare Banca	Cellulare Privato	
HO01390			BP - Responsabile Organizzazione	GUIDOLIN	RUGGERO					
HO00702			BP - Responsabile del Personale	SPEZIOTTO	ROBERTO					
GS01311			SGS - Responsabile Sicurezza di Gruppo	ANELLI	MARCELLO					
GS00110			SGS-Direttore Generale	PIETROBELLI	GIOVANNI					
HO00434			BP - Responsabile Operations	RIGODANZA	OTTAVIO					
GS00111			BCM	GOBBETTI	DALISO					

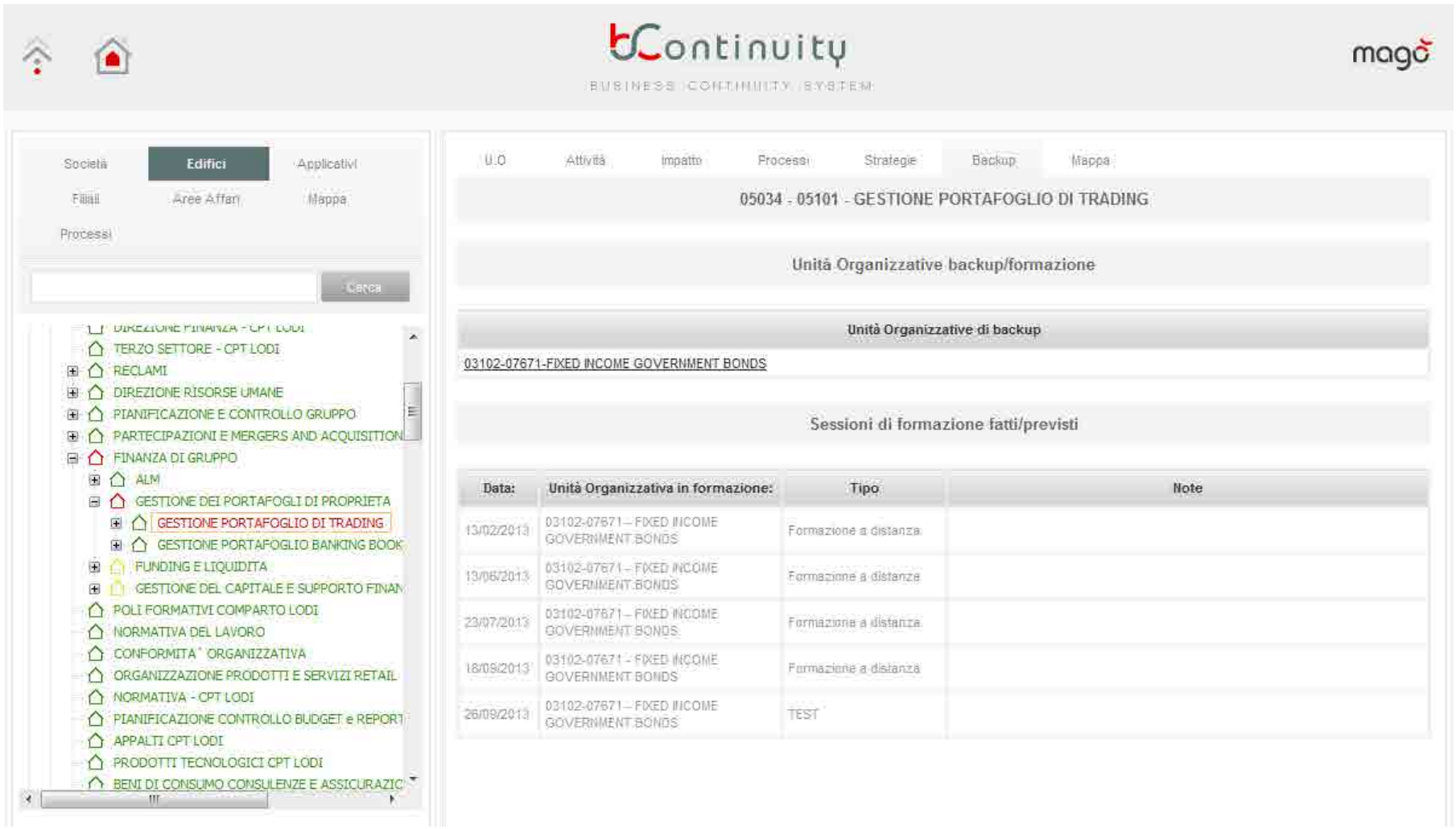
Strumento di Gestione



Strumento di Gestione

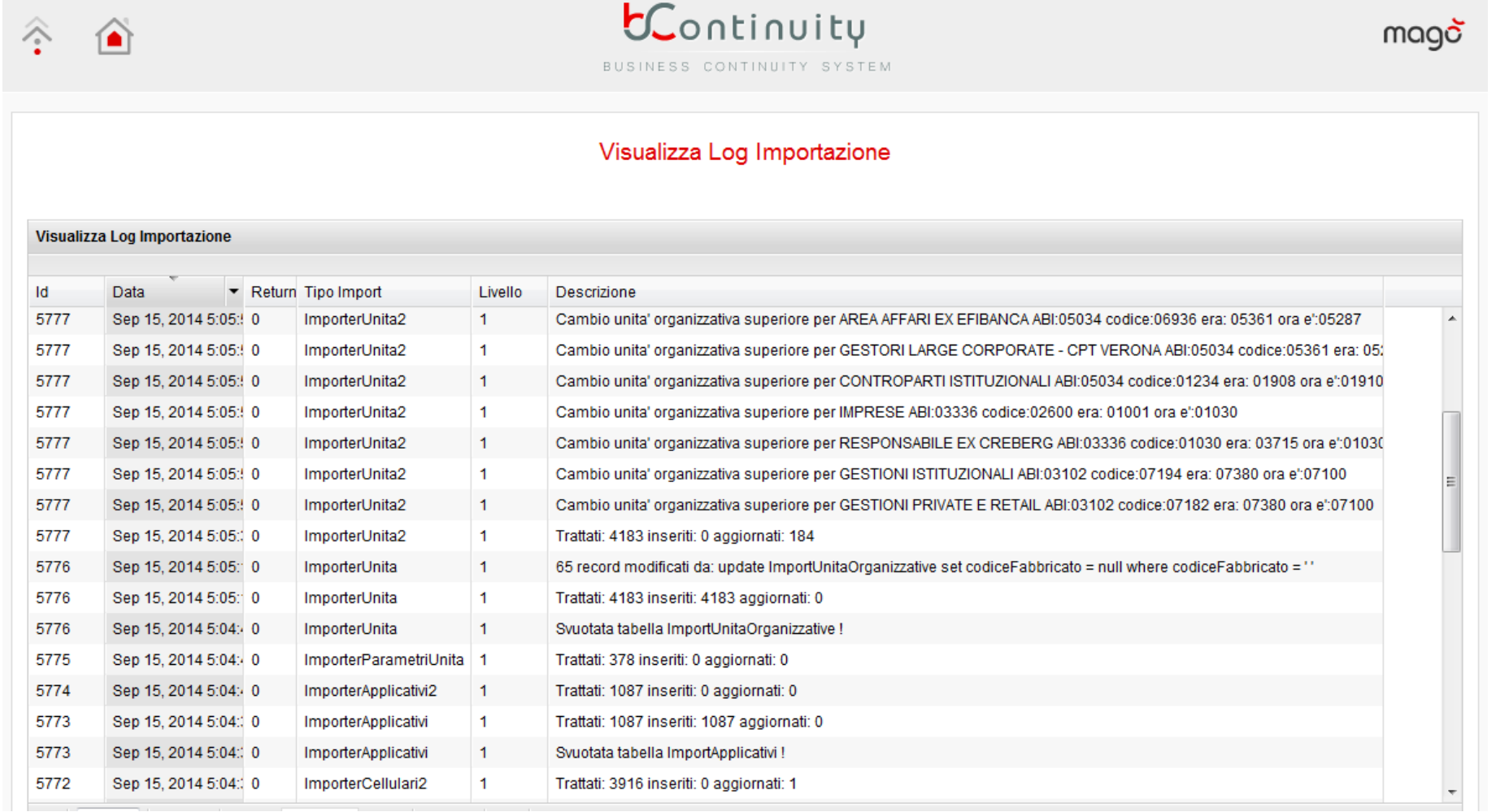


Strumento di Gestione



Strumento di Gestione

Strumento di Gestione



Id	Data	Return	Tipo Import	Livello	Descrizione
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Cambio unita' organizzativa superiore per AREA AFFARI EX EFIBANCA ABI:05034 codice:06936 era: 05361 ora e':05287
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Cambio unita' organizzativa superiore per GESTORI LARGE CORPORATE - CPT VERONA ABI:05034 codice:05361 era: 05
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Cambio unita' organizzativa superiore per CONTROPARTI ISTITUZIONALI ABI:05034 codice:01234 era: 01908 ora e':01910
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Cambio unita' organizzativa superiore per IMPRESE ABI:03336 codice:02600 era: 01001 ora e':01030
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Cambio unita' organizzativa superiore per RESPONSABILE EX CREBERG ABI:03336 codice:01030 era: 03715 ora e':0103
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Cambio unita' organizzativa superiore per GESTIONI ISTITUZIONALI ABI:03102 codice:07194 era: 07380 ora e':07100
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Cambio unita' organizzativa superiore per GESTIONI PRIVATE E RETAIL ABI:03102 codice:07182 era: 07380 ora e':07100
5777	Sep 15, 2014 5:05:5	0	ImporterUnita2	1	Trattati: 4183 inseriti: 0 aggiornati: 184
5776	Sep 15, 2014 5:05:5	0	ImporterUnita	1	65 record modificati da: update ImportUnitaOrganizzative set codiceFabbricato = null where codiceFabbricato = ''
5776	Sep 15, 2014 5:05:5	0	ImporterUnita	1	Trattati: 4183 inseriti: 4183 aggiornati: 0
5776	Sep 15, 2014 5:04:4	0	ImporterUnita	1	Svuotata tabella ImportUnitaOrganizzative !
5775	Sep 15, 2014 5:04:4	0	ImporterParametriUnita	1	Trattati: 378 inseriti: 0 aggiornati: 0
5774	Sep 15, 2014 5:04:4	0	ImporterApplicativi2	1	Trattati: 1087 inseriti: 0 aggiornati: 0
5773	Sep 15, 2014 5:04:3	0	ImporterApplicativi	1	Trattati: 1087 inseriti: 1087 aggiornati: 0
5773	Sep 15, 2014 5:04:3	0	ImporterApplicativi	1	Svuotata tabella ImportApplicativi !
5772	Sep 15, 2014 5:04:3	0	ImporterCellulari2	1	Trattati: 3916 inseriti: 0 aggiornati: 1

BIA

definizione criteri che individuano i processi critici

a tal fine, sono considerati con particolare attenzione i processi che attengono alla gestione dei rapporti con la clientela, ivi incluse imprese e pubbliche amministrazioni, e alla registrazione dei fatti contabili.

- mappatura dei processi
- identificazione processi critici nelle banche/aziende del Gruppo

BIA

Per ciascun processo critico sono individuati:

- ❑ il responsabile
- ❑ le procedure informatiche di supporto
- ❑ il personale addetto
- ❑ le strutture logistiche interessate
- ❑ le infrastrutture tecnologiche e di comunicazione utilizzate
- ❑ definizione del livello di rischio per ogni processo

BIA

Misure previste:

- misure di prevenzione
- soluzioni di continuità operativa da attivare in caso di incidente

BIA

Rischi residui

- criteri utilizzati (tempo, perdite, scenari?)
- individuazione
- accettazione formale degli stessi

BIA

L'analisi di impatto tiene conto dei parametri caratteristici della struttura organizzativa e dell'operatività aziendale, tra cui:

- le specificità
- i profili di concentrazione geografica
- la complessità dell'attività
- grado di automazione
- le dimensioni aziendali
- l'articolazione territoriale
- il livello di esternalizzazione di funzioni rilevanti
- accentramento o decentramento di processi critici
- i vincoli derivanti da interdipendenze

BIA

RTO: *Recovery Time Objective,* indica il tempo di ripristino del servizio: è la durata di tempo e di un livello di servizio entro il quale un business process ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili;

In sintesi definisce il tempo massimo previsto per il ripristino di un ***servizio/sistema*** *per* ***l'utente finale***

RPO*: Recovery Point Objective,* indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso;

In sintesi definisce a quando risale l'ultima copia dati valida

BIA

L'RTO teorico è condizionato da molteplici fattori:

- momento in cui avviene il disastro
- da quando viene misurato:
  - dal disastro o
  - dalla dichiarazione di disastro?
- interruzione del servizio durante il batch

L'RPO teorico è condizionato da molteplici fattori:

- durata della copia
- la copia avviene a sistemi fermi?
- i sistemi per cui si producono le copie sono fra loro connessi?

BIA

"*tempo di ripristino di un processo*": periodo che intercorre fra il momento in cui l'operatore dichiara lo stato crisi e l'istante in cui il processo è ripristinato a un livello di servizio predefinito. Esso è costituito dai tempi di:

- analisi degli eventi e decisione delle azioni da intraprendere, prima di effettuare gli interventi;
- ripartenza del processo, attraverso l'attuazione degli interventi tecnici e organizzativi e la successiva verifica sulla possibilità di rendere nuovamente disponibili i servizi senza danni e in condizioni di sicurezza.

BIA

MAO (maximum acceptable outage)

time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

MTPD (maximum tolerable period of disruption)

time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

BIA

RPO (recovery point objective)

point to which information used by an activity must be restored to enable the activity to operate on resumption

RTO (recovery time objective)

period of time following an incident within which

- product or service must be resumed, or
- activity must be resumed, or
- resources must be recovered

Ruoli

Organo con funzione di supervisione strategica

Organo con funzione di gestione

Organo con funzione di controllo

Responsabile del piano di continuità operativa aziendale

Referenti dei piani settoriali

Risorse umane

Ruoli

Formalizzazione

- designazione
- compiti definiti formalmente
- documentazione delle attività svolte

L'attività svolta e le decisioni assunte sono adeguatamente documentate.

Ruoli

Organo con funzione di supervisione strategica

a) stabilisce gli obiettivi e le strategie di continuità operativa del servizio;

b) assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati;

c) approva il piano di continuità operativa e le successive modifiche a seguito di adeguamenti tecnologici ed organizzativi, accettando i rischi residui non gestiti dal piano di continuità operativa;

d) è informato, con frequenza almeno annuale, sugli esiti dei controlli sull'adeguatezza del piano nonché delle verifiche delle misure di continuità operativa;

e) nomina il responsabile del piano di continuità operativa;

Ruoli

Organo con funzione di gestione

f) promuove lo sviluppo, il controllo periodico del piano di continuità operativa e l'aggiornamento dello stesso a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti;

g) approva il piano annuale delle verifiche delle misure di continuità operativa ed esamina i risultati delle prove documentati in forma scritta.

Ruoli

Organo con funzione di controllo

ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del piano di continuità operativa.

Ruoli

Responsabile del piano di continuità operativa aziendale

- ha una posizione gerarchico – funzionale adeguata
- cura lo sviluppo del piano di continuità operativa
  - ✓ ne assicura l'aggiornamento nel continuo, a fronte di cambiamenti organizzativi o tecnologici rilevanti
  - ✓ ne verifica l'adeguatezza, con cadenza almeno annuale
- tiene i contatti con la Banca d'Italia in caso di crisi

il suo nominativo è segnalato a Banca d'Italia, tra le "cariche rilevanti a fini di Vigilanza" previste nella procedura "organi sociali" (Or.So.)

Ruoli

Referenti dei piani settoriali

coordinano, per gli aspetti di competenza:

- i lavori per la definizione e la manutenzione dei piani
- l'attuazione delle misure previste nello stesso
- la conduzione delle verifiche
- definiscono le opportune modifiche dei piani, prima dell'attivazione di nuovi sistemi o processi operativi

Ruoli

Risorse umane

È individuato il personale essenziale per assicurare la continuità operativa dei processi critici

- ❑ sono fornite allo stesso indicazioni dettagliate sulle attività da porre in essere in caso di crisi
- ❑ accede alla lista di contatto e alla documentazione necessaria per operare in situazione di crisi
- ❑ ha dimestichezza con i siti alternativi
- ❑ con le apparecchiature in essi contenute
- ❑ partecipa alle sessioni di verifica delle misure di continuità operativa.

Ruoli

Risorse umane

Formazione del personale:

- Il personale coinvolto nel piano di continuità operativa è addestrato sulle misure di continuità operativa
  - ✓piano di formazione
  - ✓evidenze delle presenze

Formazione del personale

La formazione del personale in tema di Business Continuity **è necessaria,** oltre che per rispondere in modo compiuto alla normativa di Vigilanza ed alle best practice di cui abbiamo avuto conoscenza durante il corso, per **raggiungere** pienamente gli **obiettivi di Continuità** prefissati.

E' utile prevedere **tre diversi livelli** di formazione:

☞ La fruizione da parte di **tutto il personale** di un **CORSO ON LINE,** della durata variabile da circa 15 minuti a **circa 1 ora**

☞ Lo svolgimento di più sessioni di un **CORSO IN AULA** di **una giornata** destinato alle **risorse maggiormente coinvolte** nei processi rilevanti per la Business Continuity

☞ una **specifica formazione** operativa sulle **attività da compiere in caso di emergenza** deve essere **costantemente svolta** dalle **risorse direttamente impegnate** nei processi rilevanti

CORSO ON LINE

Obiettivi

Divulgare la consapevolezza e sensibilizzare le risorse di tutta l'azienda sulle tematiche di Business Continuity affrontate nel quotidiano dalla business unit.

1) Sensibilizzare le persone alla tematica della Businenss Continuity
2) Illustrare il percorso intrapreso dalla Banca per costituire un processo finalizzato alla continuità operativa
3) Trasmettere le istruzioni necessarie per affrontare eventuali situazioni di crisi

Caratteristiche

- è di carattere informativo e sintetico
- è rivolto a tutta la popolazione dell'azienda
- Prevede la possibilità di essere usufruito entro 12-18 mesi dalla data di attivazione dell'on line
- è previsto un test finale e il rilascio certificato di fruizione
- tempo massimo di impegno per lettura e test finale, 15-60 min

CORSO IN AULA

Destinatari

Responsabili e risorse chiave delle strutture individuate nell'ambito dei processi rilevanti per la Business Continuity, coinvolti per una giornata con un test finale di apprendimento

Obiettivi

accrescere la consapevolezza macro e micro sul tema Business Continuity, con un approfondimento sugli aspetti normativi e sui processi operativi di gestione della crisi

Contenuti:

- ✓ Perché dotarsi di un Piano di Continuità Operativa, come è fatto e cosa contiene
- ✓ Accrescere la sensibilità alle tematiche di Business Continuity nell'operatività quotidiana
- ✓ Le attività da porre in essere in caso di emergenza: non si può pensare di «fare tutto», ma quanto necessario ed opportuno
- ✓ Come l'Azienda ha definito la strategia di individuazione dei processi "rilevanti", le Unità Organizzative che li erogano e le strutture deputate all'intervento in caso di emergenza
- ✓ Chi dichiara la crisi, come si viene informati, come comportarsi (come NON comportarsi)
- ✓ I test: se non si prova, non si è preparati; basta poco per essere preparati, ma può costare tantissimo non esserlo

FORMAZIONE SPECIFICA

Destinatari

Le risorse che operativamante intervengono in caso di crisi a svolgere attività e/o compiti normalmente non di loro competenza

Obiettivi

Aumentare e rafforzare la conoscenza delle attività da mettere in atto, per consentire un adeguato grado di “confidenza” nell’esecuzione dei compiti assegnati

Contenuti:

- ✓ Lavoro svolto in ambiente di produzione
- ✓ Utilizzo di “Manuali Operativi” predisposti per operare in caso di crisi
- ✓ Costante monitoraggio da parte dei process owner
- ✓ Verifica della corretta funzionalità degli strumenti utilizzati

Ruoli

Audit (verifica)

- Il piano di continuità operativa
- il relativo processo di aggiornamento
- prende visione dei programmi di verifica
- assiste alle prove
- ne controlla i risultati, proponendo modifiche al piano di continuità operativa sulla base delle mancanze riscontrate. In tale ambito, particolare attenzione è posta all'analisi dei criteri di *escalation*

Ruoli

Audit (verifica)

- in caso di incidenti verifica la congruità dei tempi rilevati per la dichiarazione dello stato di crisi
- è coinvolto nel controllo dei piani di continuità operativa dei fornitori di servizi esternalizzati e degli altri fornitori critici; può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali, indipendenti e trasparenti quanto ai risultati dei controlli
- esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali

Fornitori / Outsourcer

Identificazione fornitori

- Infragruppo
- Esterni

Tipologia

- Processi critici
- Utilities
- Infoprovider
- Istituzionali
- Infrastrutture ICT
- Infrastrutture DR

Fornitori / Outsourcer

Adeguamento Contratti

- ❖ livelli di servizio assicurati in caso di crisi
- ❖ soluzioni di continuità operativa (adeguati al conseguimento degli obiettivi aziendali e coerenti con le prescrizioni della Banca d'Italia)
- ❖ modalità di partecipazione (diretta o per il tramite di comitati utente) ai test
- ❖ modalità di comunicazione in caso di incidenti
- ❖ previsioni contrattuali nel caso in cui ci siano più aziende servite dallo stesso fornitore, specie se nella stessa area geografica

Previsione di fornitori alternativi

Fornitori / Outsourcer

Audit

✓ è coinvolto nel **controllo dei piani di continuità operativa** dei fornitori di *servizi esternalizzati* e degli altri fornitori critici; può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali, indipendenti e trasparenti quanto ai risultati dei controlli

✓ **esamina i contratti** per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali

Fornitori / Outsourcer

Principi generali e requisiti particolari

Le banche che ricorrono all'esternalizzazione di funzioni aziendali presidiano i rischi derivanti dalle scelte effettuate e mantengono la capacità di controllo e la responsabilità sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento.
La decisione di ricorrere all'*outsourcing* per lo svolgimento di determinate funzioni aziendali (anche non importanti) è coerente con la politica aziendale in materia di esternalizzazione.

Fornitori / Outsourcer

In linea con il principio di proporzionalità, tale politica stabilisce almeno:

- il processo decisionale per esternalizzare funzioni aziendali (livelli decisionali; funzioni coinvolte; valutazione dei rischi, inclusi quelli connessi con potenziali conflitti di interesse del fornitore di servizi, e l'impatto sulle funzioni aziendali; valutazione dell'impatto in termini di continuità operativa; criteri per la scelta e la *due diligence* del fornitore);
- il contenuto minimo dei contratti di *outsourcing* e i livelli di servizio attesi delle attività esternalizzate;
- le modalità di controllo, nel continuo e con il coinvolgimento della funzione di revisione interna, delle funzioni esternalizzate;
- i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni aziendali di controllo la piena conoscenza e governabilità dei fattori di rischio relativi alle funzioni esternalizzate;
- i **piani di continuità operativa** (clausole contrattuali, piani operativi, ecc.) in caso di non corretto svolgimento delle funzioni esternalizzate da parte del fornitore di servizi.

Fornitori / Outsourcer

nell'accordo scritto tra la banca e il fornitore di servizi sono formalizzati e chiaramente definiti:
a) i rispettivi diritti e obblighi; i **livelli di servizio attesi**, espressi in termini oggettivi e misurabili, nonché le informazioni necessarie per la verifica del loro rispetto; gli eventuali conflitti di interesse e le opportune cautele per prevenirli o, se non possibile, attenuarli; le condizioni al verificarsi delle quali possono essere apportate modifiche all'accordo; la durata dell'accordo e le modalità di rinnovo nonché gli impegni reciproci connessi con l'interruzione del rapporto;
b) i livelli di servizio assicurati in caso di emergenza e le **soluzioni di continuità compatibili con le esigenze aziendali e coerenti con le prescrizioni dell'Autorità di vigilanza**. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.
Sono inoltre previste clausole risolutive espresse che consentano alla banca di porre termine all'accordo di esternalizzazione in presenza di eventi che possano compromettere la capacità del fornitore di garantire il servizio oppure quando si verifichi il mancato rispetto del livello di servizio concordato;

Fornitori / Outsourcer

il fornitore di servizi:
a) dispone della competenza, della capacità e delle autorizzazioni richieste dalla legge per esercitare, in maniera professionale e affidabile, le funzioni esternalizzate;
b) informa la banca di qualsiasi evento che potrebbe incidere sulla sua capacità di svolgere le funzioni esternalizzate in maniera efficace e in conformità con la normativa vigente; in particolare, comunica tempestivamente il verificarsi di incidenti di sicurezza, anche al fine di consentire la pronta attivazione delle relative procedure di gestione o di emergenza;
c) garantisce la sicurezza delle informazioni relative all'attività della banca, sotto l'aspetto della disponibilità, integrità e riservatezza; in quest'ambito, assicura il rispetto delle norme sulla protezione dei dati personali.

Fornitori / Outsourcer

la banca:
a) conserva la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi con l'esternalizzazione, inclusi quelli derivanti da potenziali conflitti di interessi del fornitore di servizi; in tale ambito, individua, all'interno della propria organizzazione, un responsabile del controllo delle singole funzioni esternalizzate dotato di adeguati requisiti di professionalità ("referente per le attività esternalizzate");
b) acquisisce i piani di continuità operativa del fornitore di servizi o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità realizzate all'interno;

Verifiche

- **Modalità di svolgimento**
- **Risorse coinvolte**
  - ✓ Persone
  - ✓ Edifici
  - ✓ Sistemi
  - ✓ Documenti/informazioni
- **Evidenze**
- **Azioni correttive**

Verifiche

TIPO	METODOLOGIA	PARTECIPANTI	FREQUENZA	COMPLESSITA'	OBIETTIVO
Verifica teorica	❑ Audit ❑ Validazione	❑ Autori del BCP ❑ Auditor esterno	ALTA	BASSA	❑ Verifica di completezza e congruenza dei contenuti
Walk-through strutturato	❑ Scenario teorico ❑ Preparazione preliminare	❑ Autori del BCP ❑ Responsabili di Team/ UO			❑ Simulazione e validazione "aiutata" delle procedure
Tattico	❑ Simulazione preannunciata ❑ Audit	❑ Team/ UO ❑ Osservatori BCM			❑ Simulazione e validazione "aiutata" delle procedure
Simulazione	❑ Simulazione pianificata/ non pianificata	❑ Team/ UO specifici ❑ Team ICT ❑ Team di supporto ❑ Osservatori BCM	BASSA	ALTA	❑ Simulazione specifica

Tratto da "Metodologia per la realizzazione del Piano di continuità operativa" – ABI LAB

Verifiche

Verifica teorica

La verifica teorica è impostata secondo le metodologia classica di auditing e di validazione "su carta". La verifica teorica consiste in analisi di congruenza e stime dell'efficacia, rapportate a specifici scenari, di quanto definito. Al termine della verifica si progettano e implementano gli eventuali emendamenti correttivi delle carenze individuate.

Walk-through strutturato

Nel walk-through strutturato si stabilisce uno scenario di crisi, e i diversi team e Unità Organizzative percorrono ("walk-through") parallelamente le attività previste dal Piano di continuità operativa. È un'attività di simulazione di ruolo che richiede la partecipazione almeno dei responsabili dei team. Lo scenario è reso noto prima della simulazione per consentire ai partecipanti di preparare e rivedere le attività assegnate a ciascuno.

Nel corso della simulazione si verificano e documentano eventuali errori o carenze del Piano di continuità operativa.

Al termine della simulazione si progettano e implementano gli eventuali emendamenti correttivi delle carenze individuate.

Tratto da "Metodologia per la realizzazione del Piano di continuità operativa" – ABI LAB

Verifiche

Verifica tattica

Una sessione di verifica tattica consiste in una simulazione condotta come "gioco di guerra" ("war-game"). Tutti i membri dei team di ripristino sono chiamati a partecipare e ad eseguire le attività previste dal Piano di continuità operativa, comunicate in anticipo o a sorpresa, sulla base delle informazioni rese note dal coordinatore della simulazione. La simulazione deve essere impostata per riproporre il più realisticamente possibile lo scenario di crisi ipotizzato.

In genere si utilizza un "orologio accelerato" per completare le attività di 3-4 giorni in un solo giorno lavorativo; questo richiede che i team agiscano sulla base delle informazioni relative allo scenario e alle evoluzioni nella forma più immediata possibile.

Anche in questo caso il BCP è verificato per eventuali errori, incongruenze o carenze. Al termine della verifica si progettano e implementano gli eventuali emendamenti correttivi delle carenze individuate.

Simulazione

Richiede l'esecuzione di parti specifiche del Piano di continuità operativa. La comunicazione, le procedure operative, l'uso di hardware/software, l'eventuale ricorso a siti alternativi, e le operazioni per garantire risultati efficaci sono necessari, ma solo limitatamente agli specifici ambiti considerati.
Gli esercizi di simulazione possono essere condotti unitamente alla compilazione di checklist per l'identificazione di eventuali modifiche ai piani e/ o all'addestramento del personale.

Tratto da "Metodologia per la realizzazione del Piano di continuità operativa" – ABI LAB

Verifiche

- Test degli impianti
- Test dei componenti
- Test del sistema informativo (test di DR)
- Test di indisponibilità delle unita critiche/edifici
- Test di terzi
  - ✓ collegamento a siti alternativi
  - ✓ partecipazione diretta come auditor
  - ✓ partecipazione come comitati utenti
  - ✓ raccolta di evidenze
- Piano dei test

Verifiche

- **Test degli impianti (sito primario e di DR)**
  - ✓ impianto elettrico
  - ✓ rete
  - ✓ connettività esterna
  - ✓ continuità elettrica (avviamento, autonomia, apparati serviti…)
  - ✓ condizionamento
  - ✓ controllo accessi e videosorveglianza

- **Evidenze delle attività di manutenzione**

Verifiche

Manutenzione U.P.S.
Filiale : CENTRO SERVIZI DEL [redacted]

RILIEVI SU U.P.S.
Ditta : [redacted]

OPERAZIONI SETTIMANALI

U.P.S. n.	Assorb. fase R	Assorb. fase S	Assorb. fase T	Tensione	Note e segnalazioni
UPS 1 A	149 A	135 A	151 A	402 V	
UPS 1 B	162 A	134 A	146 A	400 V	
UPS 1 C	149 A	138 A	138 A	400 V	
UPS 2 A	153 A	143 A	145 A	403 V	
UPS 2 B	145 A	132 A	137 A	406 V	
UPS 2 C	148 A	136 A	139 A	403 V	
UPS 3	18 A	14 A	11 A	394 V	
UPS 4	0 A	0 A	0 A	396 V	
UPS 5	0 A	0 A	1 A	400 V	
UPS 6 A	0 A	0 A	0,6 A	231 V	
UPS 6	0 A	0 A	4 A	230 V	
UPS Bunker rilancio	20,2 A	23,9 A	20,7 A	398,6 V	

Annotazioni :

Data 03/09/2014 Firma [redacted]

Verifiche

Test degli impianti

continuità elettrica edifici con processi critici (verifica degli apparati serviti, verifica illuminazione di emergenza…)

Test su alta affidabilità (alta disponibilità)

Test

- Verifica periodica sui singoli componenti
- Test effettivi di attivazione del servizio (nel caso questo non fosse già sempre attivo)
- …

La mancanza di attenzione per alcuni dei componenti prima descritti può portare all'attivazione del DR

Test su alta affidabilità (alta disponibilità)

Esempi

- Verifica che non ci siano ostacoli alle valvole di rilevazione incendio o alle bocchette antincendio
- Verifica che non siano presenti nel CED o nelle immediate vicinanze scatole o altro materiale infiammabile
- ...

Test Disaster Recovery

Indisponibilità

- CED primario
- connettività a CED primario

Test Business Continuity

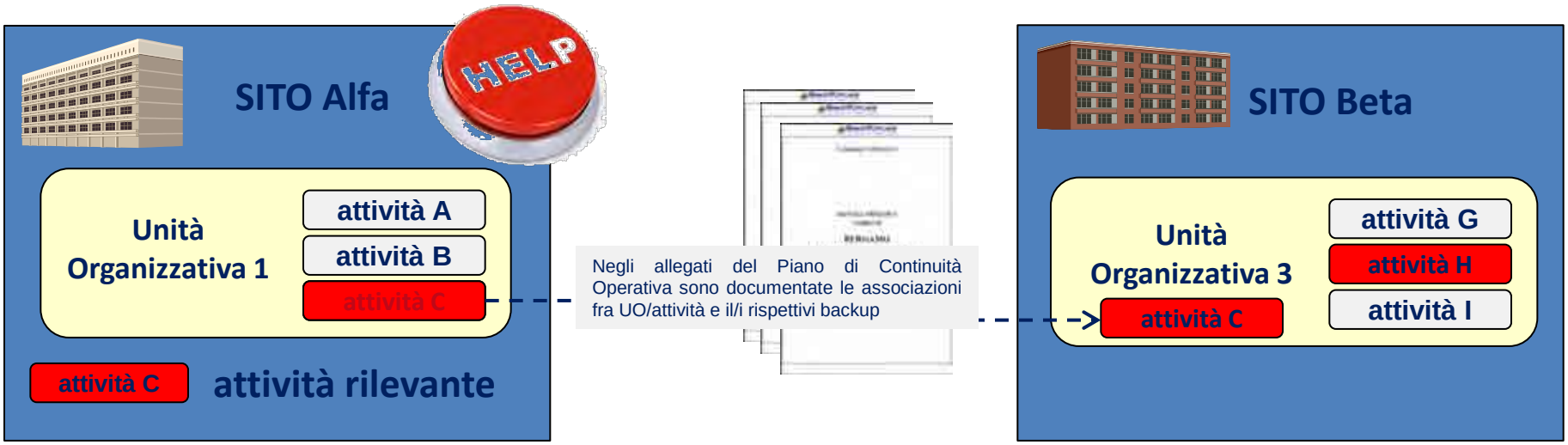
Indisponibilità:

- ❑ edifici
- ❑ personale che supporta processi critici
- ❑ sistema informativo che supporta i processi critici, compresi prodotti di produttività individuale, (ad esempio per mancanza di connettività)
- ❑ infoprovider

Esempi di Test

Esempi di Test

scenario peggiore: indisponibilità del sito e delle risorse

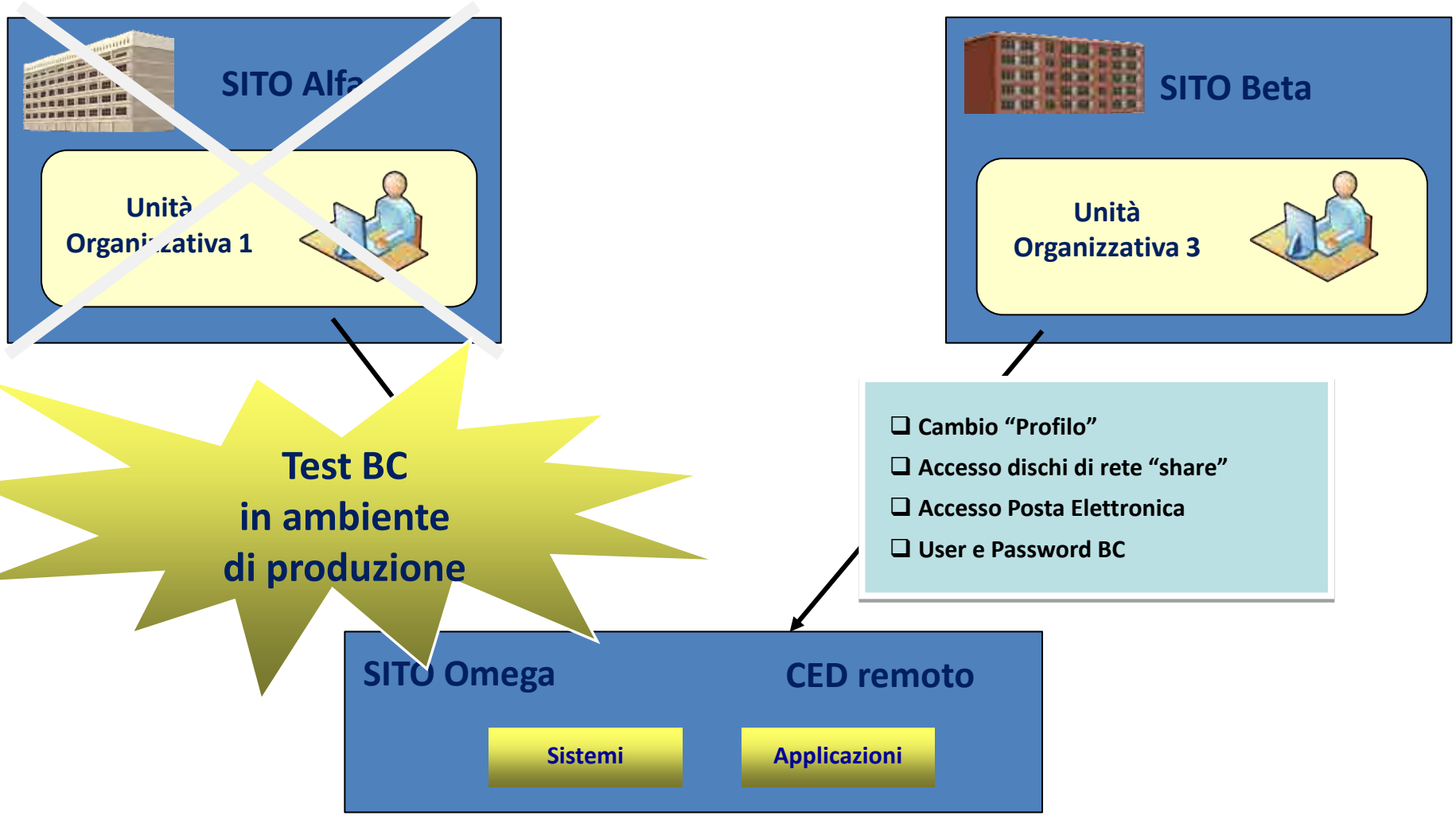


- In fase di analisi, si valutano le attività vitali svolte dalla Unità Organizzative nei vari siti e si individuano le UO che possono eventualmente agire in loro conto in caso di necessità. Le associazioni vengono definite sulla base della **localizzazione fisica** (città diversa), degli **skill del personale**, della **conoscenza del processo** (es. coinvolte a valle od a monte).

- Le Unità di backup sono oggetto di opportuna **formazione**

Esempi di Test

viene reindirizzato l'accesso al sistema informativo



Esempi di Test

Nell'ambito della Direzione Sicurezza di Gruppo si è convenuto di effettuare un test congiunto tra Safety (81/08) e Business Continuity, simulando quanto avverrebbe in caso di reale emergenza in un edificio

La data di effettuazione della prova viene mantenuta riservata

Alle 10 circa del mattino viene dato l'allarme evacuazione nell'edificio

Il personale si raduna nei punti di raccolta, tutti i colleghi sono in salvo

La Funzione Business Continuity viene informata, come previsto dalle procedure di allarme

I responsabili delle Unità Organizzative interessate vengono informati che nell'occasione si ricorre a quanto indicato nel Piano di Continuità Operativa

Viene convocata in conference call l'Unità di Crisi che, informata dal BCM dell'evento in corso, decide di avviare il test annuale

Le quattro Unità Organizzative di backup, poste in tre diverse città, sono allertate e forniscono i riferimenti operativi necessari

Tramite posta elettronica intranet sono attivate le strutture sistemistiche ed applicative del Gruppo che attuano gli interventi previsti

Esempi di Test

Business Continuity Testing : simulation of unplanned outage of the Mercato Monetario Office

Due to an unplanned event, the Mercato Monetario Office is not operative. If there is any urgent requirement, all the destinees of this communication are kindly requested to contact the Settlement Forex Money Market Office located at Lodi, telephone number + 39 037.

Comunicazione del test in corso, comprensiva dei nuovi riferimenti da contattare, viene inviata tramite posta elettronica a tutte le controparti interne al Gruppo ed esterne, italiane ed estere.

Apposita news viene pubblicata sul Portale Intranet Aziendale

Esempi di Test

Verifica e controllo dei “tempi di reazione” degli attori coinvolti e misurazione dell’intervallo temporale necessario a ripristinare le attività

Casistiche da gestire: i files lasciati aperti al momento di lasciare il posto di lavoro

Avviato lo spostamento di alcune risorse “owner” presso i siti di recovery

Coordinamento delle attività in essere e gestione di eventuali difficoltà

La Funzione di Audit presenzia al test

Il valore della pianificazione diminuisce in conformità con la complessità dello stato delle cose.

Credetemi: questo è vero. Può sembrare paradossale.

Magari pensate che più sia complessa una situazione, più è necessario un piano per poter farne fronte.

Vi concedo la teoria. Ma la pratica è diversa.

Allen Massie, 1986 "Augustus: Memoirs of Emperor". Bodley Head

Grazie per l'attenzione

Riferimenti: *g.butti@bancopopolare.it*
giancarlo.butti@promo.it
daliso@tiscali.it

