Ing. Fabrizio Di Crosta
CONSULENZA DIREZIONALE DI IMPRESA

Convegno: LA SICUREZZA DEL LAVORO NEL XXI SECOLO: QUALI PROSPETTIVE?

Ricordo del Prof. Ing. Werther Neri

giovedì 17 novembre 2016 - ore 14.00

Sala AGORA' (ex Aula Magna) Fondazione Aldini Valeriani
Via Bassanelli 9/11 – Bologna

EVENTI SISMICI:
PREVENZIONE, PROTEZIONE, SICUREZZA, EMERGENZA

La sicurezza delle informazioni in caso di sisma, calamità naturali e non naturali

I danni collaterali in caso di terremoto

La priorità è salvare le vite umane...

Poi è importante mantenere l'agibilità degli edifici ...

Ma tra i danni collaterali occorre considerare il blocco dei sistemi informativi!

La ripresa dipende anche dalla disponibilità di dati e sistemi informativi

I danni collaterali in caso di terremoto

- I danni del terremoto non si limitano alla perdita di vite umane, ai feriti, ai senza tetto e alla distruzione di immobili pubblici e privati, di ponti, strade ecc.
- Vi sono effetti collaterali con possibili gravi ripercussioni sia per la gestione dei soccorsi, per la ricostruzione e per la ripresa delle attività lavorative e sociali.
- Uno degli effetti più problematici è il **blocco dei sistemi informativi degli enti e delle aziende coinvolte nel terremoto** o in altri eventi disastrosi come frane, alluvioni, incendi, inondazioni, frane, tsunami, eruzioni vulcaniche, attentati terroristici, ecc.

È un problema di continuità operativa

La continuità operativa

La **continuità operativa** è

l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale.

La sfera di interesse della continuità operativa va oltre il solo ambito informatico, interessando l'intera funzionalità di un'organizzazione ed è assimilabile all'espressione "***business continuity***".

La Continuità Operativa

La continuità operativa comprende sia gli aspetti strettamente organizzativi, logistici e comunicativi che permettono la prosecuzione delle funzionalità di un'organizzazione, sia la continuità tecnologica, che riguarda l'infrastruttura informatica e telecomunicativa (ICT) ed è nota come "*disaster recovery*" (DR).

Le soluzioni per garantire la continuità dei servizi **non considerano soltanto le componenti tecnologiche** utilizzate, ma anche tutte le altre risorse (personale, impianti, infrastrutture, ecc.).

Le soluzioni tecniche

Esistono diversi rimedi per cautelarsi:

- **Ridondanza** dei dati
- **Protezione fisica** dei *data center*/centri elaborazione dati
- **Backup**
- **Cloud storage**
- Procedure di ***disaster recovery***
- ***….***

Il Business Continuity Plan

La Metodologia

Soprattutto le diverse tecniche vanno adottate in modo pianificato, dopo aver valutato attentamente

- I **rischi** che si corrono
- Quale **livello di servizio** si intende ripristinare
- **Entro quanto tempo** si desidera riprendere l'attività

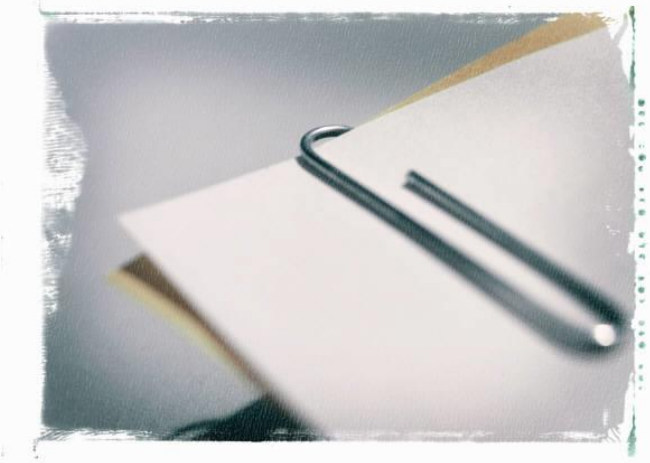
Business Continuity Plan

Business Continuity Management

Il Piano di Continuità Operativa

Per mantenere la business continuity va definito cosa fare, come farlo e con quali risorse...

...occorre definire un **Piano di Business Continuity** (Piano di Continuità Operativa)



Il Business Continuity Plan: perché serve

Molti sono gli esempi di situazioni critiche – essenzialmente causate da disastri naturali – che non sono state fronteggiate nel modo corretto e che hanno portato a costi sociali elevatissimi che si sono scaricati inevitabilmente sulla collettività:

Il Business Continuity Plan: perché serve

Il terremoto dell'Aquila 2009, dell'Emilia 2012, del Centro Italia 2016

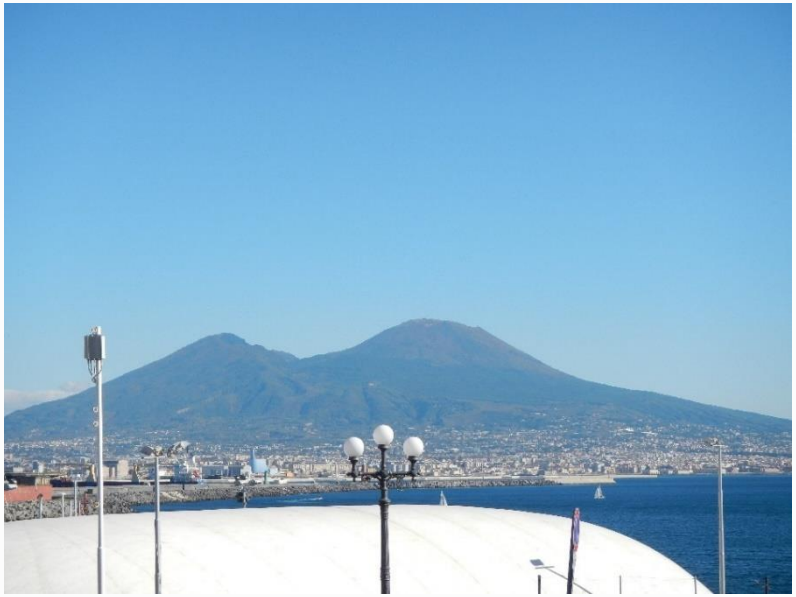
Le alluvioni in Liguria ed in Toscana

Il Business Continuity Plan: perché serve

Le interruzioni di energia elettrica protrattesi nel tempo a Cortina qualche Natale fa e, più recentemente, in Emilia dopo una forte nevicata

Il Business Continuity Plan: perché serve

Altri eventi disastrosi e distruttivi che minacciano la sicurezza dei dati potrebbero verificarsi e causare gravi conseguenze



Il Business Continuity Plan

In tutte queste situazioni di emergenza, oltre ai danni materiali ed alle perdite di vite umane, si sono verificate disfunzioni e ritardi nella **ripresa dell'operatività ordinaria**.

Il vantaggio di avere predisposto un buon piano di continuità operativo è proprio questo: ipotizzando una situazione di crisi si cerca di **limitare i danni** e di **tornare all'operatività normale nel più breve tempo possibile**.

Il BCP secondo le norme ISO

- la **ISO 27001** tratta la continuità operativa in termini di sicurezza delle informazioni, ovvero per **garantire il ritorno alla piena disponibilità delle informazioni senza perdite significative delle stesse**,
- la **ISO 22301** amplia il raggio di azione del *business continuity plan*, comprendendo la **gestione delle discontinuità di un servizio**, non necessariamente legato alla disponibilità di informazioni su supporto cartaceo o elettronico (anche se oggi ben poche attività possono farne a meno).

La sicurezza dei data center

Esistono schemi per la certificazione della sicurezza dei data center attraverso la valutazione del design, della costruzione e dell'operatività della **struttura del DC** in relazione alle seguenti tematiche:

scelta della sede - progettazione della sicurezza - requisiti tecnici - requisiti strutturali - requisiti organizzativi - gestione degli eventi - documentazione del DC - sicurezza delle informazioni - conformità legislativa - efficienza energetica.

La sicurezza dei Data Center

Progettazione del DC

Costruzione del DC

Collaudo

Conduzione del DC

Certificazione

- UpTime
- EN 50600
- DC Maturity Model
- Schema TUV Intercert
- …

La norma ISO 22301: certificazione della business continuity

Lo standard **ISO 22301 (*Societal security — Business continuity management systems — Requirements***) specifica i requisiti per progettare, implementare e gestire efficacemente un **Sistema di gestione della continuità operativa**.

Dal 2016 è disponibile anche la versione in italiano con la

UNI EN ISO 22301:2014 Sicurezza della società - Sistemi di gestione della continuità operativa - Requisiti

La norma ISO 22301: certificazione della business continuity

Scopo della norma per la gestione della *business continuity* è quello di **specificare i requisiti atti a pianificare, stabilire, implementare, realizzare, monitorare, riesaminare, mantenere e migliorare in modo continuo un sistema di gestione documentato per proteggersi contro gli incidenti che possono accadere e fermare l'organizzazione**,

ma non solo...

il BCMS ha anche l'obiettivo di **ridurre la probabilità che tali eventi negativi avvengono, prepararsi ad essi e rispondere in modo adeguato per ripristinare l'operatività nel più breve tempo possibile** qualora l'incidente che causa lo stato di crisi si verifichi.

La norma ISO 22301: certificazione della business continuity

Il sistema di gestione della continuità operativa (*business continuity management system* o BCMS) enfatizza l'importanza di:

- **comprendere le esigenze dell'organizzazione** e le necessità per stabilire la politica e gli obiettivi di un sistema di gestione per la continuità del business
- **implementare e rendere operativi controlli e misure** per gestire la capacità di un'intera organizzazione nella gestione delle interruzioni dell'operatività dovute a cause accidentali
- **monitorare e riesaminare le prestazioni** e l'efficacia del sistema di gestione della continuità operativa
- del **miglioramento continuo** del BCMS basato su obiettivi misurabili.

La norma ISO 22301: certificazione della business continuity

La ISO 22301 evidenzia i componenti chiave del sistema di gestione della continuità operativa, peraltro presenti anche in altri sistemi di gestione. Tra essi:

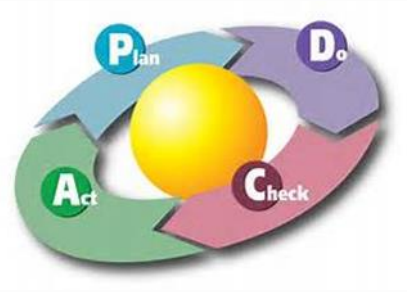
- la **politica**
- le **persone** con le loro **responsabilità** definite
- la **gestione dei processi** correlati a politica, pianificazione, attuazione ed operatività del BCMS
- **valutazione delle prestazioni**
- **riesame della direzione** e **miglioramento**
- la **documentazione** in grado di fornire evidenze verificabili tramite **audit** sul sistema di gestione della continuità operativa

La norma ISO 22301: certificazione della business continuity

Anche la ISO 22301introduce il metodo del "**PLAN DO CHECK ACT"** già noto da altre norme dei sistemi di gestione.

Il modello PDCA del sistema di gestione della continuità operativa ha come input

- le **parti interessate** (clienti, proprietà/soci, dipendenti/collaboratori, fornitori, collettività) e i **requisiti per la business continuity**



mentre l'output del sistema

- è fornito alle stesse parti interessate ed è costituito dalla **continuità operativa gestita**.

La norma ISO 22301: certificazione della business continuity

Sono fornite le classiche definizioni legate alla **gestione del rischio** (risk assessment, risk management, rischio) tra cui il *risk appetite,* ovvero la **propensione al rischio** dell'organizzazione che, dovrà essere identificata al fine di intraprendere azioni di prevenzione idonee.

Dovranno essere documentati i collegamenti tra la **politica per la continuità operativa** e gli **obiettivi dell'organizzazione** e la sua politica, inclusa una **strategia generale di gestione dei rischi** e l'approccio dell'organizzazione ai rischi correlati alla *business continuity*, ovvero la propria **propensione al rischio**.

La norma ISO 22301: certificazione della business continuity

Aspetti trattati:

- **pianificazione e controllo** dei processi operativi
- **valutazione dei rischi**
- l'analisi di impatto, ovvero la ***business impact analysis*** (BIA)
- la **strategia di business continuity**, ovvero tutto ciò che l'organizzazione intende fare per garantire la continuità operativa, compresa la definizione dei ***business continuity plan*** o piani di continuità operativa, la loro applicazione e test.

La norma ISO 22301: certificazione della business continuity

- Le modalità di effettuazione e documentazione della ***business impact analysis*** e della **valutazione del dei rischi**, per la quale può essere preso come riferimento quanto indicato nella ISO 31000 (**UNI ISO 31000 – Gestione del rischio - Principi e linee guida**).

La norma ISO 22301: certificazione della business continuity

Occorre precisare che sia l'analisi di impatto sia la valutazione dei rischi dovranno prendere in considerazione i **rischi che possono impattare la continuità operativa**, quindi i rischi che si verifichino **incidenti distruttivi** che portino a **situazioni di crisi** o comunque di interruzione dell'operatività e, conseguentemente, a situazioni insostenibili per la **propensione al rischio** definita per l'organizzazione.

A fronte di tali situazioni, in base ai risultati della valutazione dei rischi, dovranno essere determinate e poste in essere le **azioni conseguenti per mantenere la continuità operativa**.

Normative di riferimento per la business continuity

Le principali normative sull'argomento richiamate esplicitamente o implicitamente dalla ISO 22301 sono le seguenti:

ISO 22300, *Societal security — Terminology*

UNI CEI ISO/IEC 27001, Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti

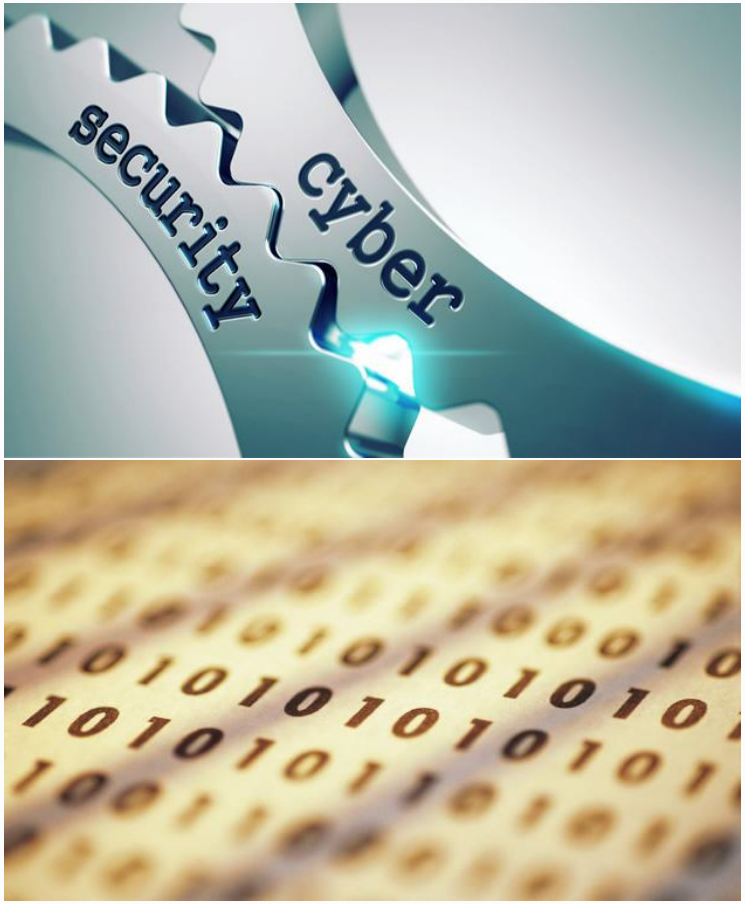
ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

BS 25999-1, *Business continuity management — Code of practice*

BS 25999-2, *Business continuity management — Specification*

UNI ISO 31000 – Gestione del rischio - Principi e linee guida

Business continuity ICT



Anche la norma ISO/IEC 27031 "*Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*" tratta la business continuity, ma nel contesto dell'ICT e delle tecniche di sicurezza strettamente correlata alla ISO 27001 che contiene i **requisiti per la certificazione dei sistemi di gestione della sicurezza delle informazioni**.

Sicurezza delle Informazioni: Il giusto equilibrio fra tre aspetti

ISO 27000

17/11/2016
MEMORIAL PROF. W. NERI - LA SICUREZZA DELLE INFORMAZIONI IN CASO DI SISMA
31

Il Business Continuity Plan ISO 27001

Il BCP (*Business Continuity Plan*) o **Piano di Continuità Operativa** è un documento richiesto alle **organizzazioni certificate ISO 27001** (*Sistema di gestione per la sicurezza delle informazioni* - Requisiti) al punto di controllo

A.17 «Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa»

ed ai controlli

- **A.17.1 «Continuità della sicurezza delle informazioni»**
- **A.17.2 «Ridondanze»**

Il Business Continuity Plan ISO 27001

A.17.1 «Continuità della sicurezza delle informazioni»

- **Obiettivo: La continuità della sicurezza delle informazioni dovrebbe essere integrata nei sistemi per la gestione della continuità operativa dell'organizzazione.**
- A.17.1.1 Pianificazione della continuità della sicurezza delle informazioni
- A.17.1.2 Attuazione della continuità della sicurezza delle informazioni
- A.17.1.3 Verifica, riesame e valutazione della continuità della sicurezza delle informazioni

Il Business Continuity Plan ISO 27001

- **A.17.2 «Ridondanze»**
- **Obiettivo: Assicurare la disponibilità delle strutture per l'elaborazione delle informazioni.**
- A.17.2.1 Disponibilità delle strutture per l'elaborazione delle informazioni

Tali controlli sono dettagliati nella UNI CEI ISO/IECISO 27002 - Tecnologie informatiche - Tecniche per la sicurezza Raccolta di prassi sui controlli per la sicurezza delle informazioni

Il Business Continuity Plan

Le analisi, valutazioni e scelte di trattamento del rischio richieste dalla gestione della continuità operativa sono le seguenti:

- Identificazione dei rischi
- Analisi e valutazione dei rischi
- Analisi delle conseguenze di disastri, malfunzionamenti, interruzioni di servizi (*Business Impact Analysis*)
- Realizzazione di piani (controlli) affinché i processi di business siano riattivati entro il tempo richiesto

Il Business Continuity Plan

Le analisi valutano per ogni *asset* (o gruppo di *asset*) critico il tempo che tale *asset* può rimanere indisponibile con danno basso o nullo.

I piani (*Business Continuity Plan*) devono essere mantenuti costantemente aggiornati per essere efficaci al momento del bisogno.

Il Business Continuity Plan

Il processo di gestione della continuità operativa deve prendere in esame tutti i processi e le attività aziendali e classificarli in funzione della loro criticità

Attività critiche per il business (MCA's)

Attività importanti

Attività secondarie

Il Business Continuity Plan

Per meglio comprendere la predisposizione di un BCP occorre introdurre alcune definizioni basilari:

Mission Critical Activity (MCA): attività critica o di supporto al business relativamente ai servizi o prodotti offerti dall'organizzazione (internamente o esternamente), incluse le sue correlazioni con altri processi e *single points of failure*, che permettono all'organizzazione di raggiungere i suoi obiettivi di business considerando le stagionalità e/o tempi di rilascio critici

Il Business Continuity Plan

Business Impact Analysis (BIA): analisi gestionale attraverso la quale un'organizzazione valuta quantitativamente (per esempio finanziariamente, *Service Level Agreement*, SLA) e qualitativamente (per esempio reputazione, leggi, regolamenti) gli impatti e le perdite che possono risultare se l'organizzazione subisce un grave incidente, e il minimo livello di risorse necessarie per il ripristino.

Il Business Continuity Plan

Maximum Acceptable Outage (MAO) ovvero il tempo massimo ritenuto accettabile che può trascorrere - a fronte di un evento avverso - durante il quale non viene fornito un prodotto/servizio o non viene svolta un'attività.

Maximum Tolerable Period of Disruption **(**MTPD) ovvero il tempo massimo tollerabile che può trascorrere a fronte degli impatti negativi conseguenti ad un incidente come risultato della mancata fornitura di un prodotto, erogazione di un servizio o svolgimento di un'attività operativa.

Si noti che rispetto al MAO il MTPD è un periodo potenzialmente superiore in quanto si può presumere che gli impatti negativi di una interruzione di un servizio possano durare più a lungo dell'interruzione stessa.

Il Business Continuity Plan

Maximum Tollerance DownTime (MTDT): massimo intervallo di tempo ammissibile di interruzione del servizio (*quante ore posso permettermi di non erogare il servizio ai clienti?*).

Maximum Tollerance Data Loss (MTDL): massima perdita di dati tollerata (*quanti dati posso permettermi di perdere?*).

Il Business Continuity Plan

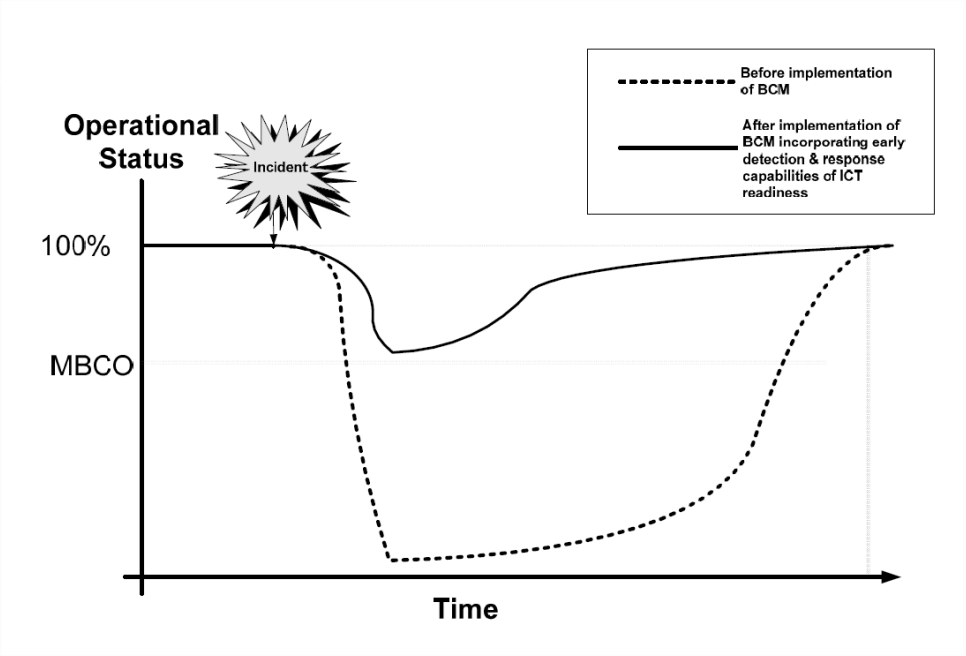
RTO (*Recovery Time Objective*): periodo di tempo entro il quale devono essere ripristinati un minimo livello di servizio, i sistemi di supporto e le funzionalità principali dopo un'interruzione dei servizi. Normalmente è il lasso di tempo entro il quale cui le MCA devono essere ripristinate.

Il Business Continuity Plan

RPO (Recovery Point Objective): istante (punto) nel tempo al quale i dati sono coerenti e possono essere ripristinati.

Il Business Continuity Plan

MBCO (*Minimum Business Continuity Objective*): livello di servizio minimo accettabile dall'organizzazione per raggiungere i propri obiettivi di business durante una rottura.

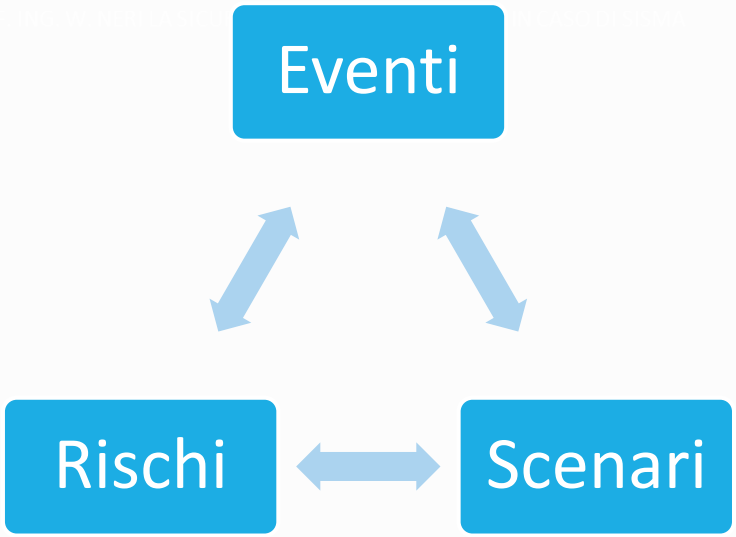


Il Business Continuity Plan

Per le **attività critiche** vengono stabiliti degli **obiettivi di continuità operativa** in termini di MTDT, MTDL, RTO, RPO, MBCO e stabiliti dei **piani di continuità operativa**, che comprendono le contromisure messe in campo per garantire gli obiettivi.

Il Business Continuity Plan

Per la pianificazione delle attività di continuità operativa è necessario valutare preliminarmente gli impatti degli eventi che possono causare interruzioni dei processi di business, predisponendo una BIA.



Il Business Continuity Plan

A seguito della **valutazione dei rischi di interruzione del servizio** erogato ai clienti devono essere predisposti, attuati e periodicamente verificati uno o più **Piani di Continuità Operativa** (*Business Continuity Plan*) aventi lo scopo di mantenere o ripristinare il funzionamento dei processi critici ed assicurare la disponibilità delle informazioni necessarie a garantire un **livello di servizio accettabile**, a fronte del verificarsi dei rischi di interruzioni o malfunzionamenti precedentemente identificati e valutati.

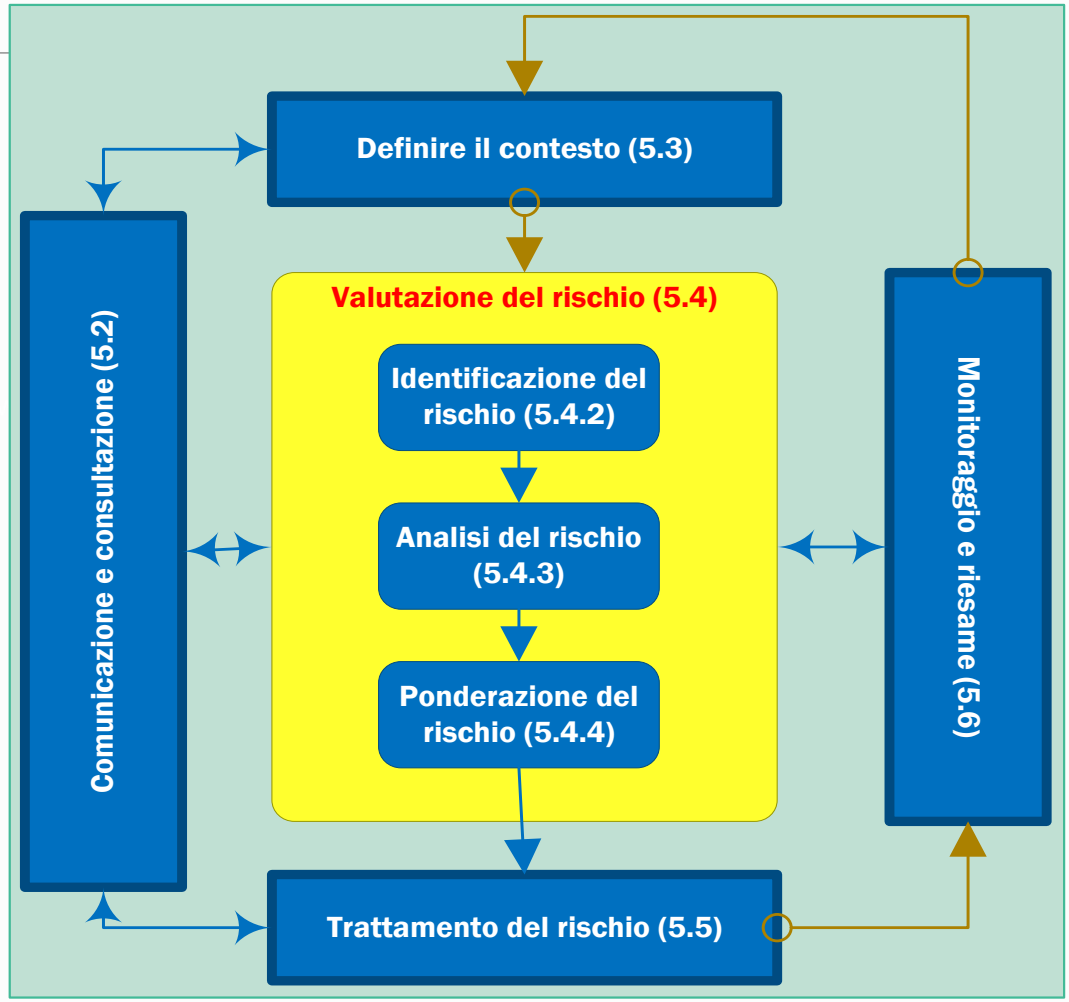
Il Business Continuity Plan

Dunque se pensiamo ad un servizio di pubblica utilità occorre definire due livelli:

1. I livello che identifica il **ripristino di un servizio minimo dopo l'interruzione**
2. II livello che sancisce la **ripresa dell'attività ordinaria**

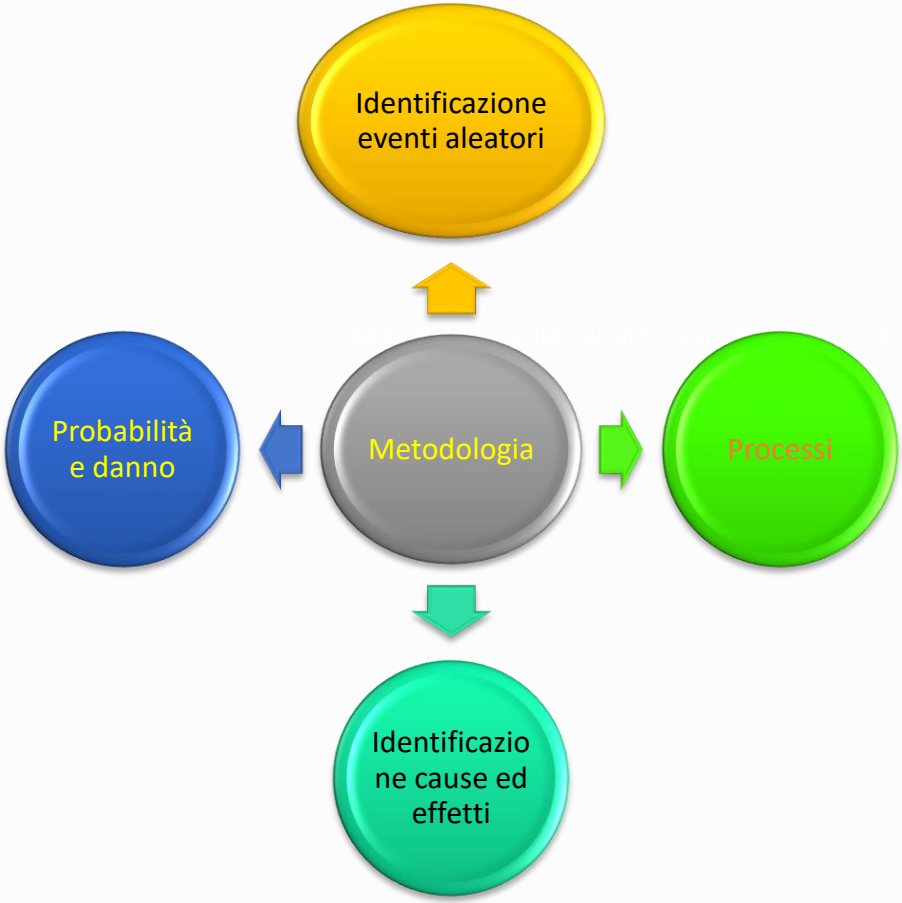
Per ogni livello devono essere stabiliti i tempi entro i quali vengono raggiunti e che possono costituire SLA contrattuali.

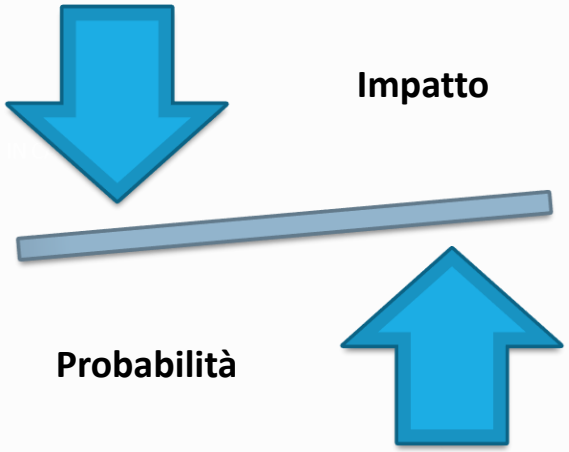
Risk Management
Il processo



Fonte UNI 12230:2007 – Fig.A.1

Risk assessment





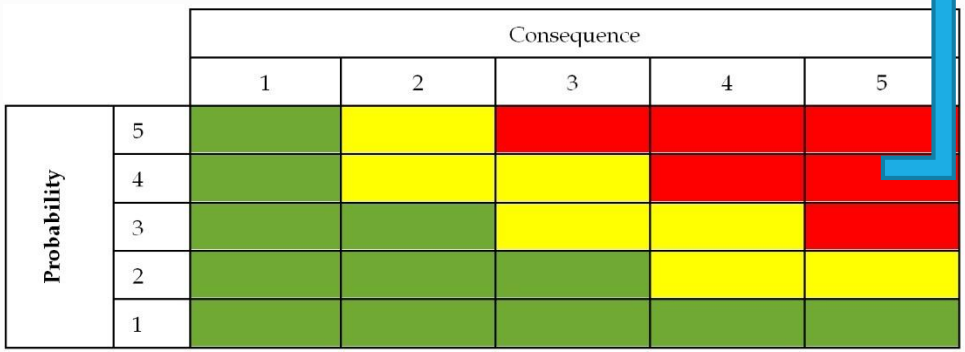
Risk management

In generale ogni metodologia prevede di:

- ✓Scomporre i processi
- ✓Analizzare gli eventi
- ✓Identificare le cause
- ✓Valutare gli effetti
- ✓Ponderare il rischio
- ✓Trattare il rischio

Trattamento del rischio

Tecniche di risk assessment



Il Business Continuity Plan

È bene comprendere che i BCP devono prefigurare uno **scenario di crisi** ben definito, al verificarsi del quale si vuole reagire in modo adeguato.

Chiaramente non tutti gli scenari possibili possono essere gestiti nei BCP, ma solo quelli **più probabili e di impatto più grave**, sulla base della valutazione dei rischi preliminarmente svolta.

Il Business Continuity Plan: contenuti

1. Scopo e campo di applicazione
2. Obiettivi
3. Requisiti di business continuity (RPO, RTO,...)
4. Identificazione dei processi critici (MCA's)
5. *Business Impact Analysis*
6. Piano di *Disaster Recovery*
7. Piano di Continuità Operativa
8. Test del BCP (prove, tempi, responsabilità)
9. Manutenzione del BCP

Il Business Continuity Plan

7) Il Piano di Continuità Operativa contiene:

- Rilevazione dell'incidente (metodi e procedure): dichiarazione del disastro o incidente, valutazione del danno, attivazione del piano)
- Risposta all'incidente (attività, tempi, responsabilità, procedure)
- Ripristino dell'operatività (attività, tempi, responsabilità, procedure di azione e continuità)

Il Business Continuity Plan

- Risorse (personale e competenze, tecnologie, infrastruttura, software, dati, siti alternativi, centri di emergenza o crisi)
- Fornitori (Lista dei fornitori di *recovery*, dettagli dei contratti, procedure di attivazione)
- Organizzazione e Responsabilità
- Documentazione
- Comunicazioni (contatti, soggetti da informare, messaggi)

Il Business Continuity Plan

I BCP possono far riferimento ad altri documenti (ad es. Piani di *Disaster Recovery*), aggiornati autonomamente.

In ogni caso deve essere sempre possibile risalire alla configurazione attuale del BCP, ovvero alle revisioni vigenti dei documenti esterni richiamati nel Piano di Continuità Operativa.

Il Business Continuity Plan

La configurazione e la relativa rintracciabilità dei documenti relativi al BCP deve essere disponibile sia in formato elettronico, sia su supporto cartaceo, con gestione di copie di riserva del BCP disponibili in locali/siti/ubicazioni alternative, al fine di essere sempre disponibili in caso di verificarsi dell'evento che ha generato l'interruzione dei processi critici.

Il Business Continuity Plan

Per la Pubblica Amministrazione la continuità operativa ed i relativi Piani di Business Continuity sono previsti dall'Art. 50 bis del Codice per l'Amministrazione Digitale; la continuità operativa, pertanto, deve essere gestita dai responsabili degli Enti Pubblici in modo adeguato, con riferimento agli standard internazionali sulla materia.

Grazie per l'attenzione

Fabrizio Di Crosta

fabrizio@dicrosta.it

www.dicrosta.it