

Il contributo AIEA al GdL sulle Emergenze Locali

Luigi Carrozzi

Coordinatore Gruppo di Ricerca AIEA sugli ISMS

Annalisa Cocco

(AIEA/BULL)

“ISCOM e AIEA Un punto di vista comune su come mettere in campo e certificare la sicurezza delle informazioni “

Sala Convegni ISCOM - 31 Gennaio 2007

Il tema: infrastrutture critiche locali e gestione delle emergenze

Una infrastruttura è critica quando:

“..una eventuale interruzione o distruzione delle sue risorse fisiche, dei suoi servizi, dei suoi sistemi di information technology, delle sue reti di comunicazione o di qualunque altro suo bene infrastrutturale comporta un serio impatto sulla salute, la sicurezza fisica, sociale, ed economica dei cittadini e sulla efficacia di funzionamento dei governi”

Focus :

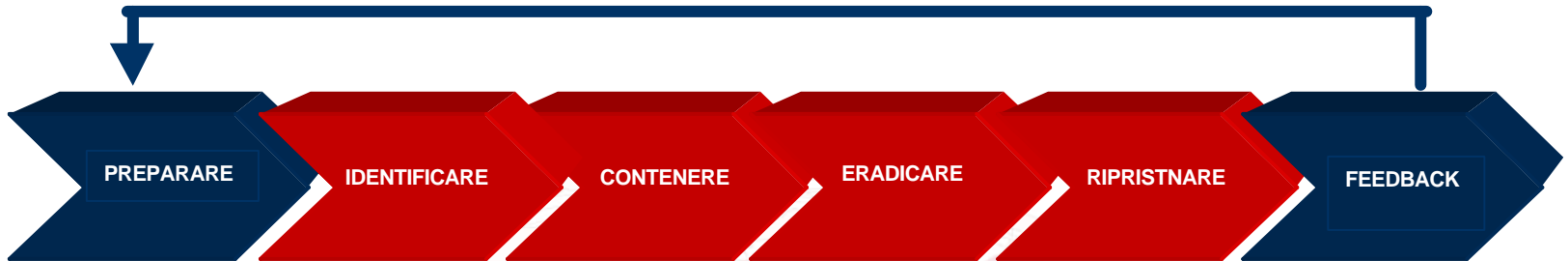
- **Aziende e organizzazioni che operano a livello locale e regionale**
- **Infrastruttura ICT (infrastrutture critiche informatizzate)**

Essere preparati a gestire le emergenze

 A large, semi-transparent, pinkish-red AIEA logo is centered on the page. It is overlaid on a faint, light-colored globe that shows the outlines of continents and latitude/longitude lines. The logo consists of the letters 'AIEA' in a bold, rounded, sans-serif font.

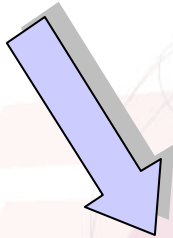
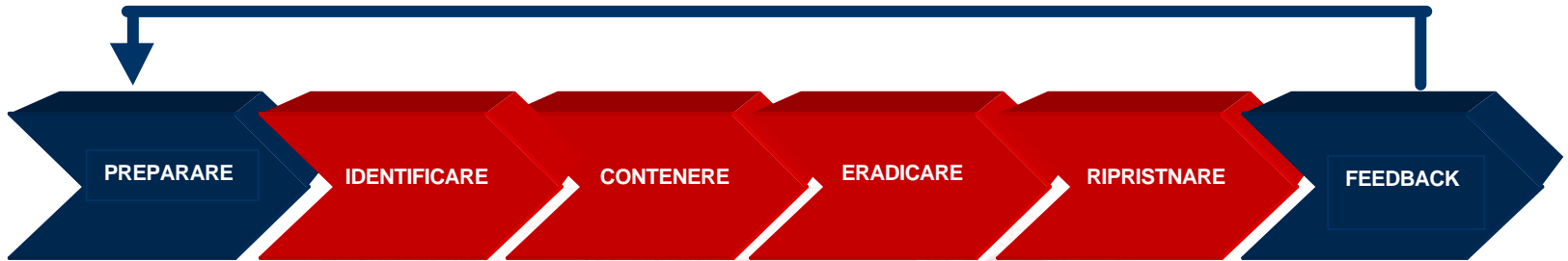
Luigi Carrozzi - Annalisa Cocco - "Il contributo AIEA al GdL sulle Emergenze Locali" - Sala Convegni ISCOM - 31 Gennaio 2007

Costituzione del sistema di gestione delle emergenze

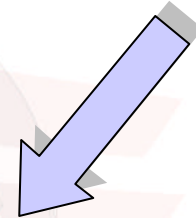
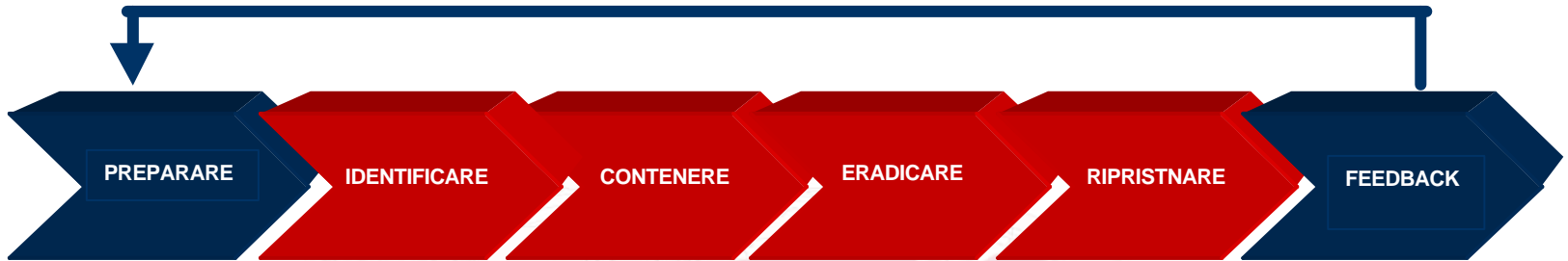


Le fasi di **preparazione** e **feedback** costituiscono il processo stesso di fondazione, generazione, crescita e mantenimento a livelli adeguati della capacità di reazione dell'organizzazione alle emergenze.

Preparare

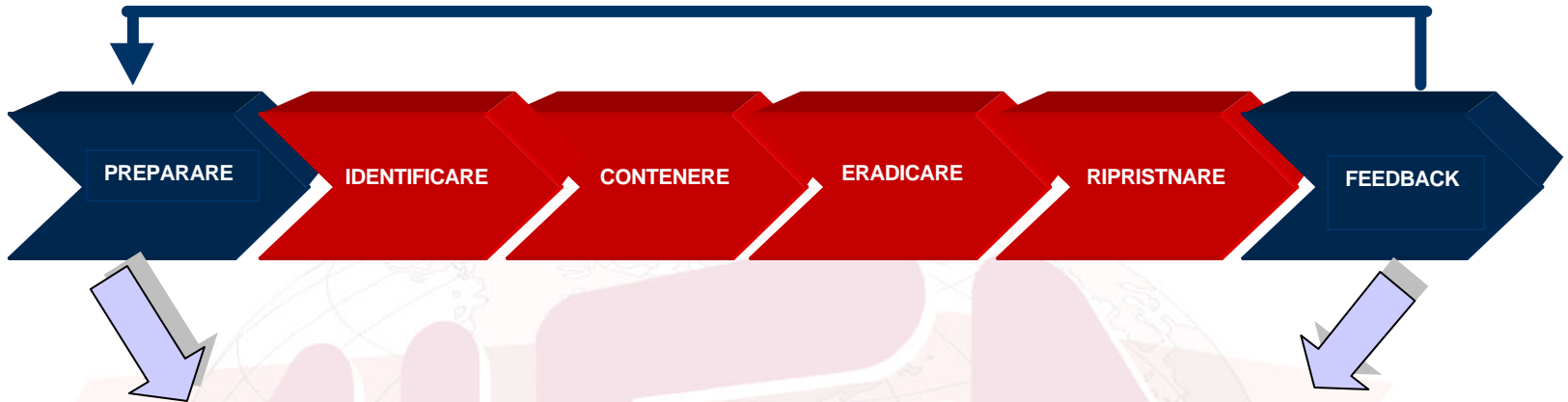


***Dominio di riferimento, asset ed obiettivi di protezione
Business Impact Analysis
Rilevazione e gestione del rischio
Policy e procedure operative
Organizzazione, ruoli e responsabilità
Allocazione di risorse (economiche, personale, mezzi e strumenti)
Formazione***



Verifica del comportamento dell'organizzazione
Verifica della validità delle policy e procedure operative
Verifica dell'idoneità delle risorse (skill, mezzi, strumenti)
Rilevazione delle variazioni di contesto dell'organizzazione
Rilevazione delle variazioni di contesto dell'ambiente
Piano di miglioramento 'sostenibile'

La sfida del miglioramento



Tali attività debbono entrare nelle **prassi operative** delle organizzazioni

E' necessario predisporre **metodologie operative destinate ad una molteplicità di operatori, facilmente adottabili, e calzate sui processi produttivi** delle diverse organizzazioni target

Aspetti definitivi e modelli di gestione

 A large, semi-transparent, pinkish-red stylized logo of the letters 'AIEA' is centered on the page. The logo is overlaid on a faint, light-colored globe that shows the outlines of continents and latitude/longitude lines. The globe is also semi-transparent, allowing the background to be seen through it.

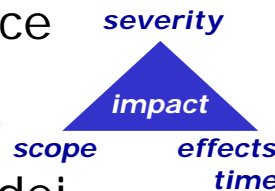
Luigi Carrozzi - Annalisa Cocco - "Il contributo AIEA al GdL sulle Emergenze Locali" - Sala Convegni ISCOM - 31 Gennaio 2007

Le aziende e le organizzazioni che operano **a livello locale** devono **comprendere e valutare il livello di criticità della loro attività**

Emergenza: situazione generalmente collegata all'indisponibilità temporanea/permanente o al malfunzionamento di risorse "critiche" che possono essere infrastrutturali e/o umane...

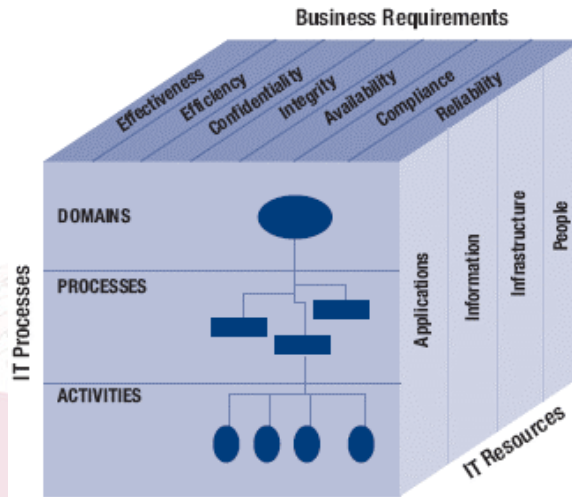


Definizione e classificazione di un evento (da semplice problema a stato di crisi) in base a: **livello di gravità, estensione e durata temporale dell'impatto** conseguente al verificarsi dell'evento ed alla valutazione dei rischi associati



Importanza del processo preventivo di **classificazione di informazioni e related information assets**

Come gestire le emergenze: la metodologia (1/2)



Fonte: COBIT v4.0, © 2005 IT Governance Institute)

La gestione delle emergenze è un **processo strategico** deve essere integrato con tutto il **ciclo di vita** di un sistema ICT

L'utilizzo di **linee guida e standard** ITZ fornisce garanzia che tutti gli aspetti siano presi in considerazione e strettamente collegati con i requisiti di business: metodologie **COBIT**-Control Objectives for Information and related Technology e **NIST**-National Institute of Standards and Technology, modello **PDCA** (Plan, Do Check, Act)

Luigi Carrozzi - Annalisa Cocco - "Il contributo AIEA al GdL sulle Emergenze Locali" - Sala Convegni ISCOM - 31 Gennaio 2007

Come gestire le emergenze: la metodologia (2/2)



In ognuna delle quattro fasi del ciclo di vita di un sistema ICT **il COBIT propone sia obiettivi di controllo** da attuare per garantire l'efficacia della gestione delle emergenze.

Come costruire il Piano per la gestione delle emergenze (1/2)

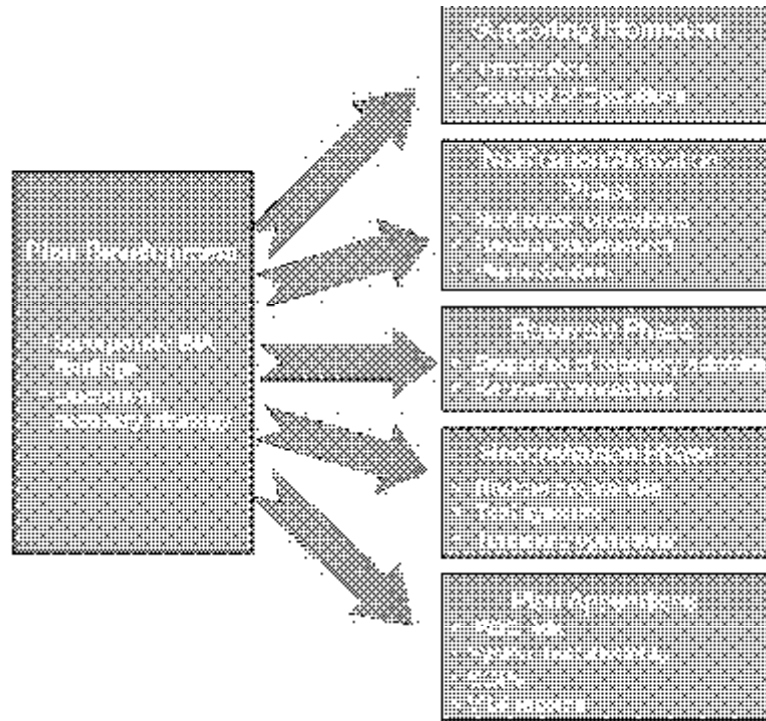


Fonte: NIST

In parallelo alla formulazione del Piano, va definita una **metrica per controllare il processo ed il raggiungimento degli obiettivi di business**

Il **COBIT** individua obiettivi di controllo per i principali processi inerenti la gestione delle emergenze

Come costruire il Piano per la gestione delle emergenze (2/2)



Fonte: NIST

Il **Piano** si compone di cinque parti fondamentali ed include i **ruoli e le responsabilità** interne ed esterne all'organizzazione per la gestione delle emergenze

Luigi Carrozzì - Annalisa Cocco - "Il contributo AIEA al GdL sulle Emergenze Locali" - Sala Convegni ISCOM - 31 Gennaio 2007