

This document is a property of FINMECCANICA Società per Azioni. Do not distribute, do not quote, and do not reproduce it, unless following FINMECCANICA written approval.

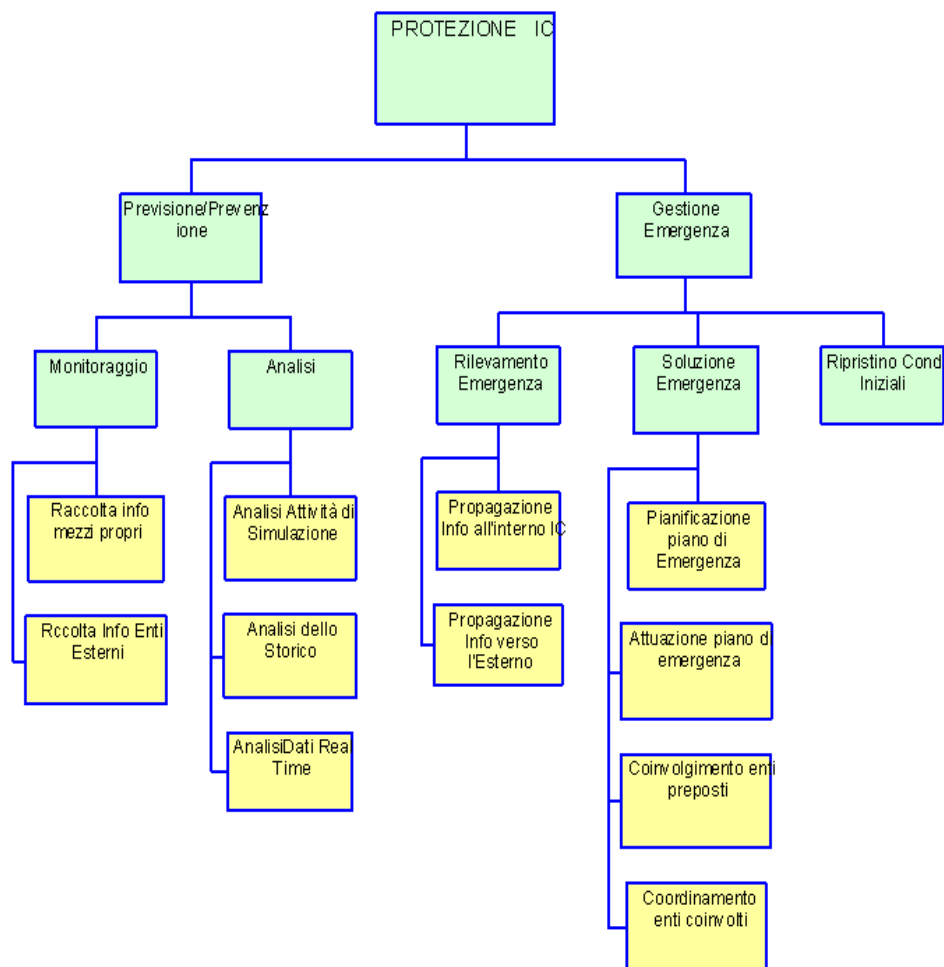
The present material has been produced for supporting an oral presentation; thus, it cannot be exhaustive if considered alone.

Sicurezza Integrata delle Infrastrutture Critiche

Roma, 15 giugno 2010

Definire un modello integrato di gestione dei rischi che consenta di valutare le principali aree di vulnerabilità, i possibili scenari di crisi e i costi/benefici di soluzione di prevenzione, protezione e ripristino





L'obiettivo per cui si definisce un Modello Operazionale è quello di identificare e descrivere secondo Standard consolidati le logiche e le modalità operative delle attività di previsione, prevenzione, protezione e ripristino delle IC, coprendo sia attività di routine sia attività di emergenza.

Analizzare le principali dinamiche di correlazione e interdipendenza fra le IC e fra le attività in carico ai gestori delle IC stesse, sia durante la normale gestione operativa che in caso di situazioni di emergenza provocate da eventi accidentali o attacchi intenzionali e definire i possibili scenari operazionali di prevenzione, protezione e ripristino

Identificare soluzioni organizzative e tecnologiche di tipo “*netcentrico*” che, a partire dalle nuove opportunità offerte in campo ICT, consentano di abilitare un modello innovativo di collaborazione interdipendente fra gli operatori dei servizi di Pubblica Utilità (PU – Public Utilities) e la interoperabilità e comunicazione tra le PU stesse ed i vari enti pubblici interessati al fine di migliorare il livello dei servizi forniti e la resilienza dei processi di prevenzione, protezione e ripristino.

Il sistema di Sicurezza Integrata Infrastrutture Critiche deve essere in grado di supportare in logica collaborativa le principali attività di:

- pianificazione,
- esercizio,
- intervento e manutenzione,
- monitoraggio e gestione

delle risorse e delle emergenze per eventi accidentali (tecnologici e naturali) o attacchi intenzionali a carico delle strutture, controllate mediante il Centro di Comando e Controllo (CEC).

Il sistema di gestione IC deve:

- poter gestire i vincoli di interoperabilità e di interdipendenza fra le diverse infrastrutture, oltre che offrire significativi spazi di miglioramento sia dei livelli di sicurezza sia nell'efficacia delle risorse investite;
- Possedere caratteristiche di scalabilità, in grado di garantire sia risultati di breve periodo, sia l'identificazione di interventi strutturali di medio - lungo periodo.

Integrazione di specifiche “capabilities” quali:

- Ausilio all’attività di gestione specifica delle strutture;
- Modellizzazione, simulazione ed analisi dei rischi e degli impatti;
- Rilevazione, identificazione e autenticazione di individui, merci e mezzi;
- Localizzazione e posizionamento;
- Sorveglianza e Protezione;
- Comunicazione;
- Statistiche e Metriche;
- Centro Comando E Controllo (CEC).

Integrazione di sensori, attuatori e sistemi informativi esterni, su modelli per l'integrazione di dati eterogenei (operatori, sistemi, aree geografiche) e sulle applicazioni di comando, coordinamento e supporto ai processi decisionali e operativi.

La soluzione deve prevedere due diversi livelli:

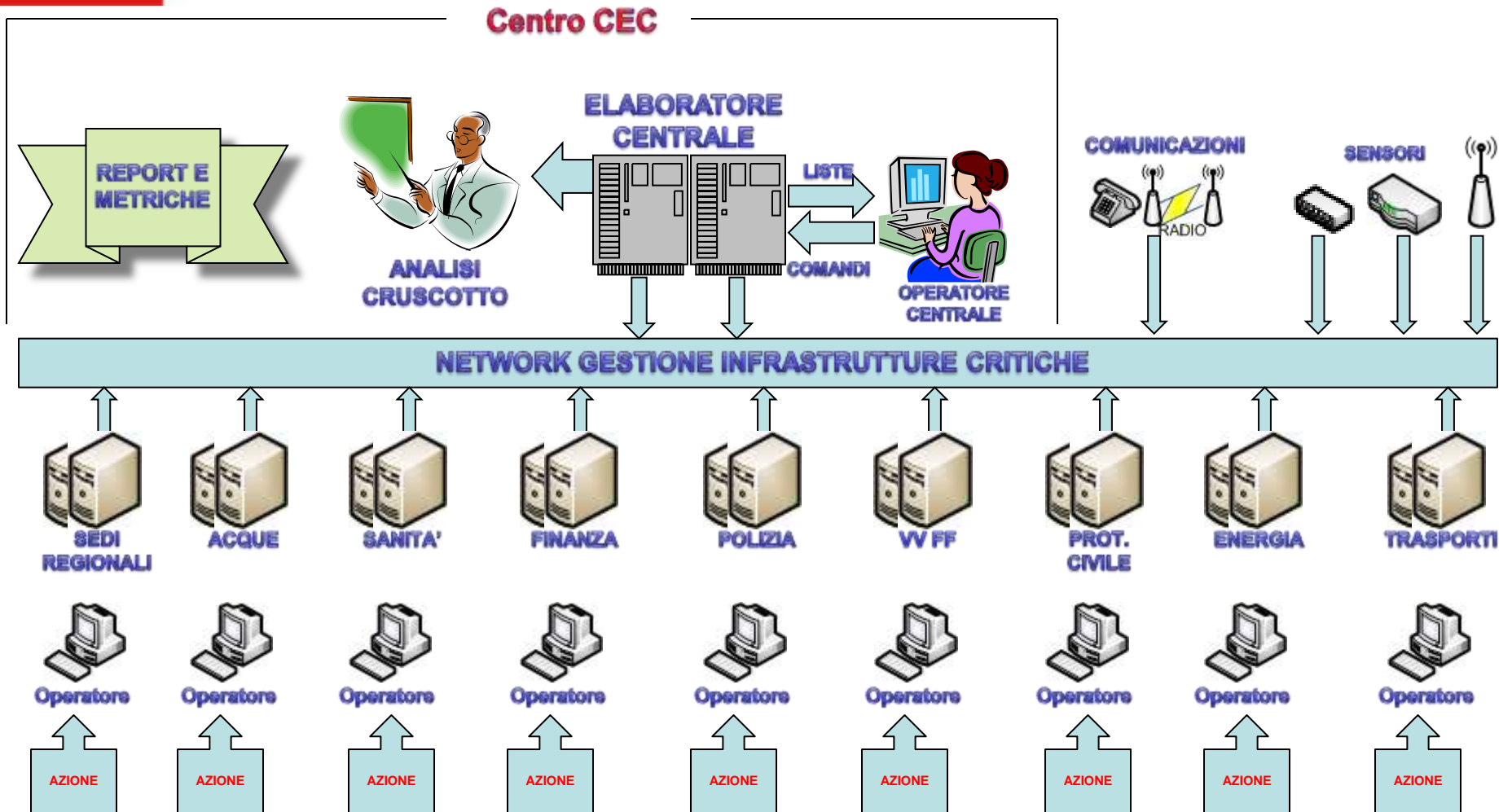
- Sistema di Sicurezza Integrata IC Nazionale;
- Sistema di Sicurezza Integrata IC Locale.

- Censimento delle caratteristiche dei principali sistemi informativi e delle rispettive soluzioni tecnologiche adottate dagli operatori di infrastrutture critiche per la gestione delle attività di manutenzione e risposta all'emergenza;
- Mappatura dei processi operativi e decisionali finalizzati alla gestione della manutenzione e alla risposta all'emergenza dei principali operatori di infrastrutture critiche (energia, trasporti, sanità, ecc.);

- Definizione di un modello operativo in cui, in coerenza con i risultati ottenuti dall'analisi di rischio, sono individuati i principali nodi di interdipendenza tra le infrastrutture critiche e i corrispondenti parametri chiave per la gestione degli scenari di disservizio o incidente;
- Predisposizione di un modello di collaborazione tra gli operatori coinvolti che comprenda aspetti di pianificazione e gestione della manutenzione e di coordinamento delle attività di risposta all'emergenza derivante, in relazione a più scenari operativi, da eventi di origine umana o naturale in grado di generare un effetto domino.

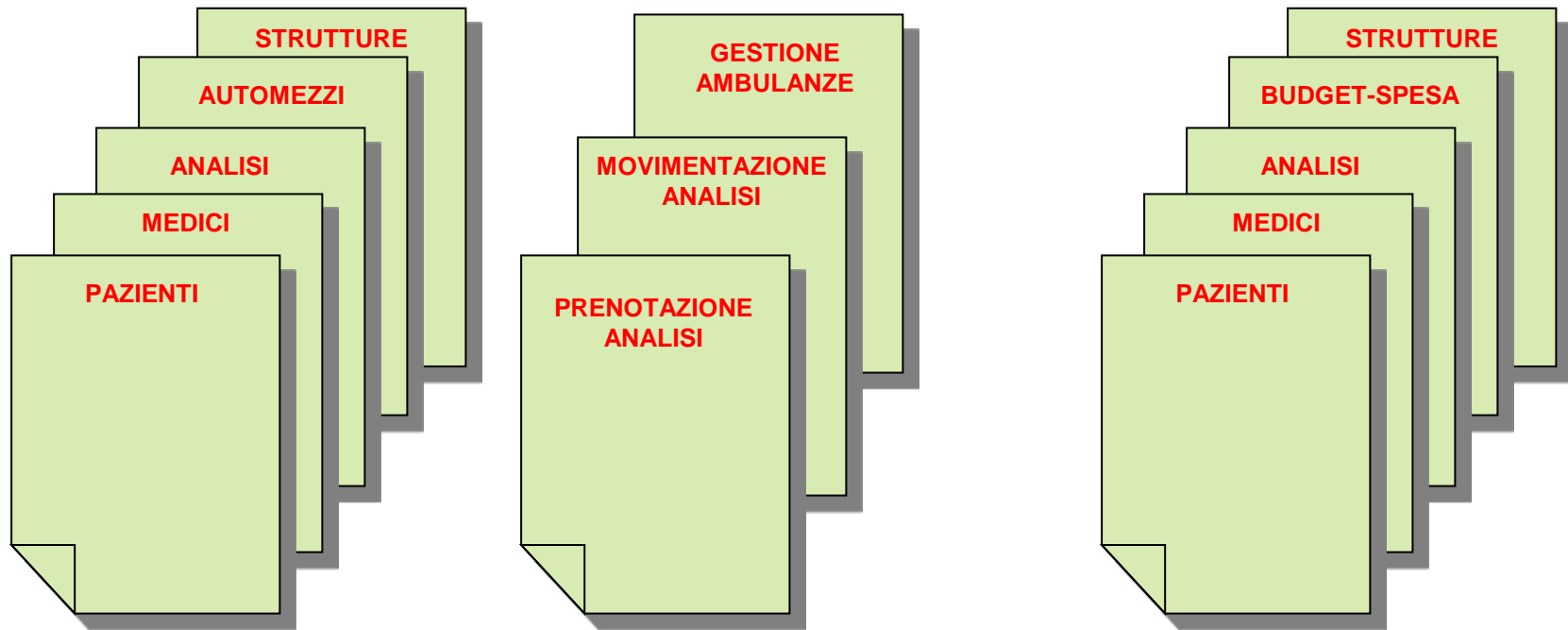
- Organizzazione (chi si occupa di gestione rischi, emergenze, copertura)
- Principali rischi identificati
- Attività di prevenzione
- Attività di emergenza
- Interdipendenze (esistenti, info desiderate, criticità)
- Relazioni con altri operatori IC (es. protocolli d'intesa, comunicazioni, etc.) e tecnologia implementativa
- Relazioni con Enti pubblici e di soccorso

Sistema Sicurezza Integrata IC Locale



Sketch funzionale - Sanità

CRUSCOTTO PERFORMANCE PRESTAZIONI & RISCHI



**Gestione
ANAGRAFICA**

**Gestione
SERVIZI**

**STATISTICHE
E
METRICHE**

Esempio di cruscotto Semaforo - Regione

SEDI REGIONALI



STATO



ULTIMO AGGIORNAMENTO

20-05-09 11:23:50 Situazione Normale

ACQUE



20-05-09 11:23:50 Situazione Normale

SANITA'



20-05-09 11:23:50 Situazione Normale

FINANZA



20-05-09 11:23:50 Situazione Normale

POLIZIA



20-05-09 11:23:50 Situazione Normale

VV FF



STATO



ULTIMO AGGIORNAMENTO

20-05-09 11:23:50 Situazione Normale

PROT. CIVILE



20-05-09 11:23:50 Situazione Normale

ENERGIA

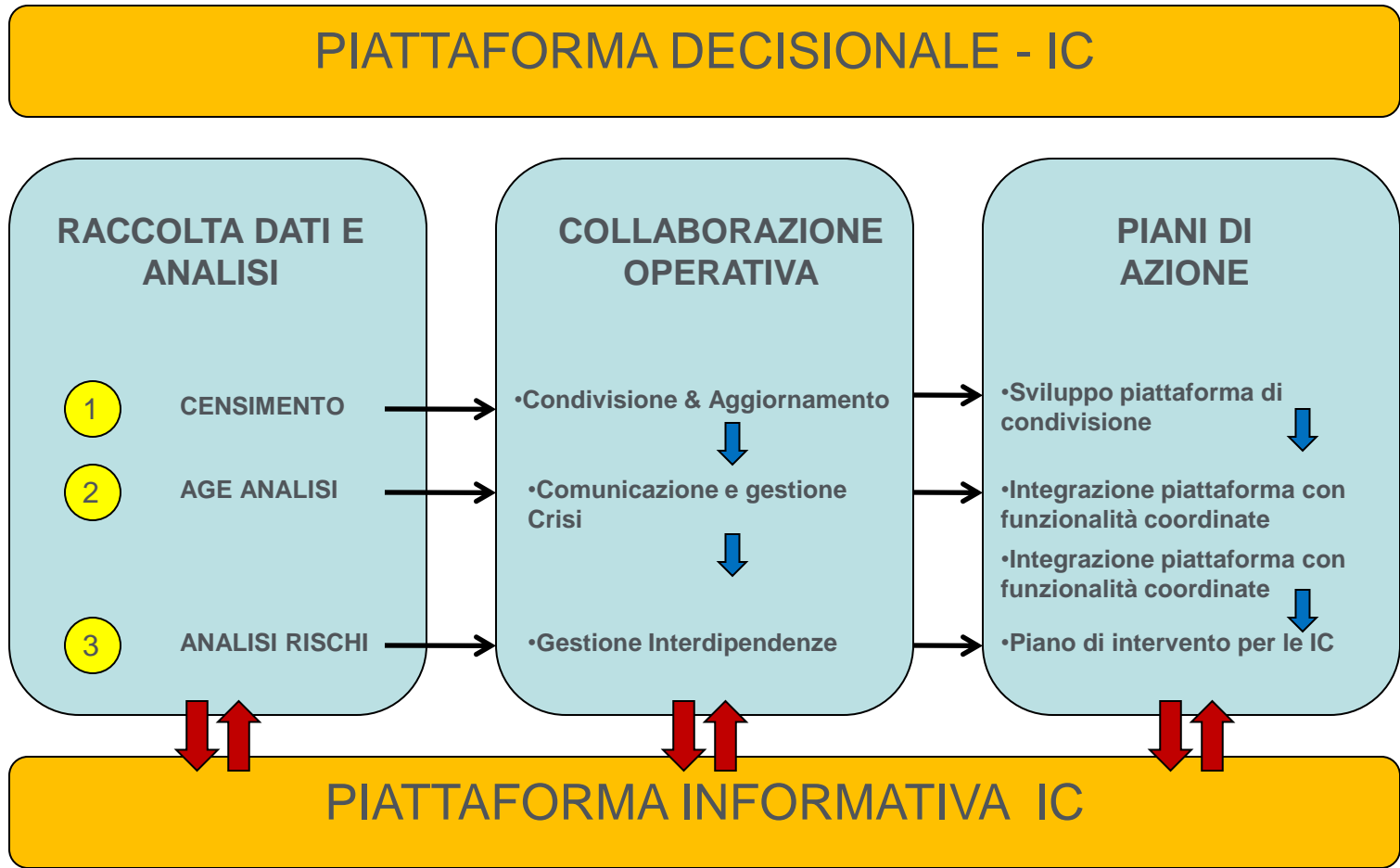


20-05-09 11:23:50 Situazione Normale

TRASPORTI



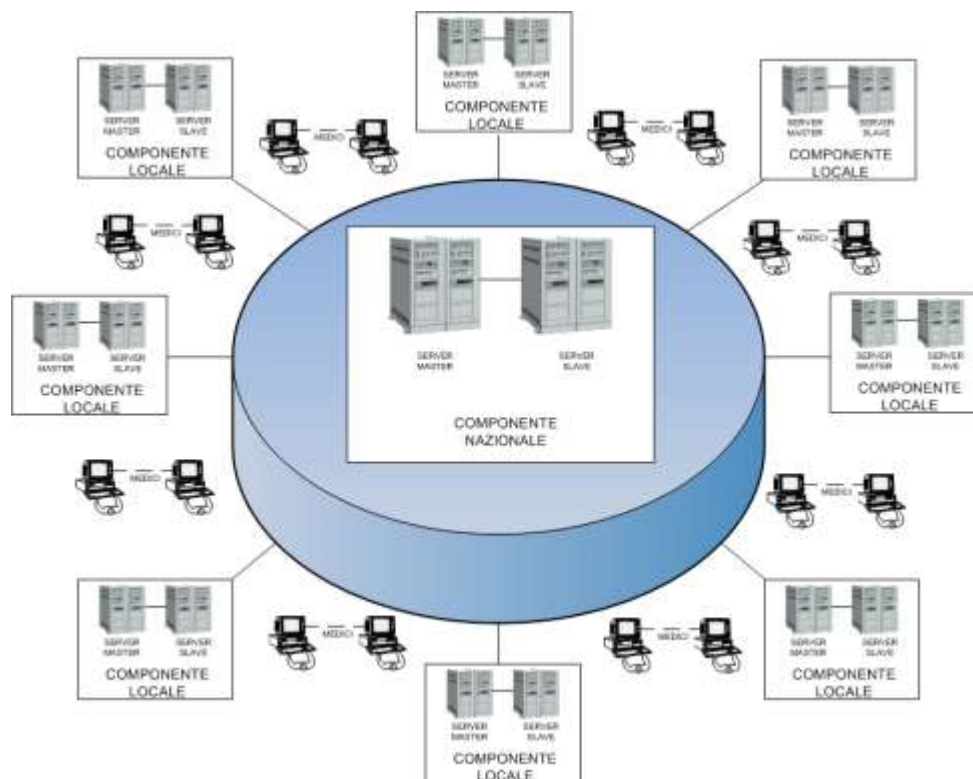
20-05-09 11:23:50 Situazione Normale



Ridondanza e Disaster Recovery

ARCHITETTURA di SISTEMA

Il sistema si basa su una architettura netcentrica ridondata a tutti i livelli e si compone di una componente Nazionale ridondata e di “n” componenti Locali anch’esse ridondate.



DISASTER RECOVERY

Tutti i dati di lavoro e/o database utilizzati per le elaborazioni peculiari di ogni componente Locale sono memorizzati anche a livello di componente Nazionale, per cui in caso di “black-out” o “disaster” Locale, la componente Nazionale è in grado di subentrare con la elaborazione Locale effettuata in ambito di sistema Nazionale, per poi restituire le funzionalità alla componente Locale, laddove la stessa venga ripristinata.

Centro Comando e Controllo



REPORT E METRICHE



MONITOR A PARETE



MONITORING

NETWORK



OPERATORE



OPERATORE



OPERATORE

- Misurazione della metrica produttiva ed individuazione delle aree critiche con particolare bisogno di correttivi da porre in atto
- Visibilità globale sullo stato delle risorse sia umane che infrastrutturali su tutto il territorio nazionale
- Maggiore ergonomia nella gestione delle varie risorse delle strutture su tutto il territorio nazionale
- Mappatura completa delle infrastrutture e siti e servizi critici con caratterizzazione dei principali rischi e fattori di vulnerabilità e obsolescenza

- Attivazione tavolo di confronto e opportunità di coordinamento tra le principali strutture coinvolte e sensibilizzazione per la mitigazione dei rischi
- Generazione di linee guida per l'ottimizzazione delle modalità di pianificazione, gestione e protezione delle infrastrutture critiche a partire dai modelli operativi e sistemi esistenti
- Sensibile miglioramento della sicurezza e dei servizi nelle strutture su tutto il territorio nazionale

Grazie per l'attenzione.



Romolo Bernardi

VP Group Security Office (GSO)

Piazza Monte Grappa, 4

00195 - Roma

Tel. +39 06 32473438

Fax + 39 06 32473508

romolo.bernardi@finmeccanica.com
