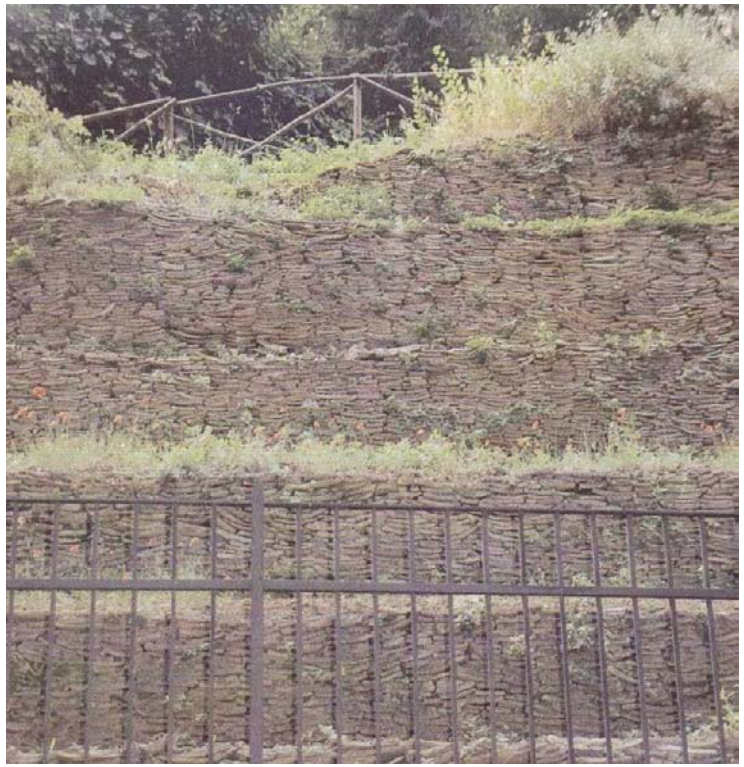
Sicurezza informatica, pianificazione e gestione delle emergenze informatiche in una Public Utility: l'esperienza di AMA

Eugenio Orlandi
AMA S.p.A. – Roma
www.amaroma.it

AMA S.p.A. : Mission

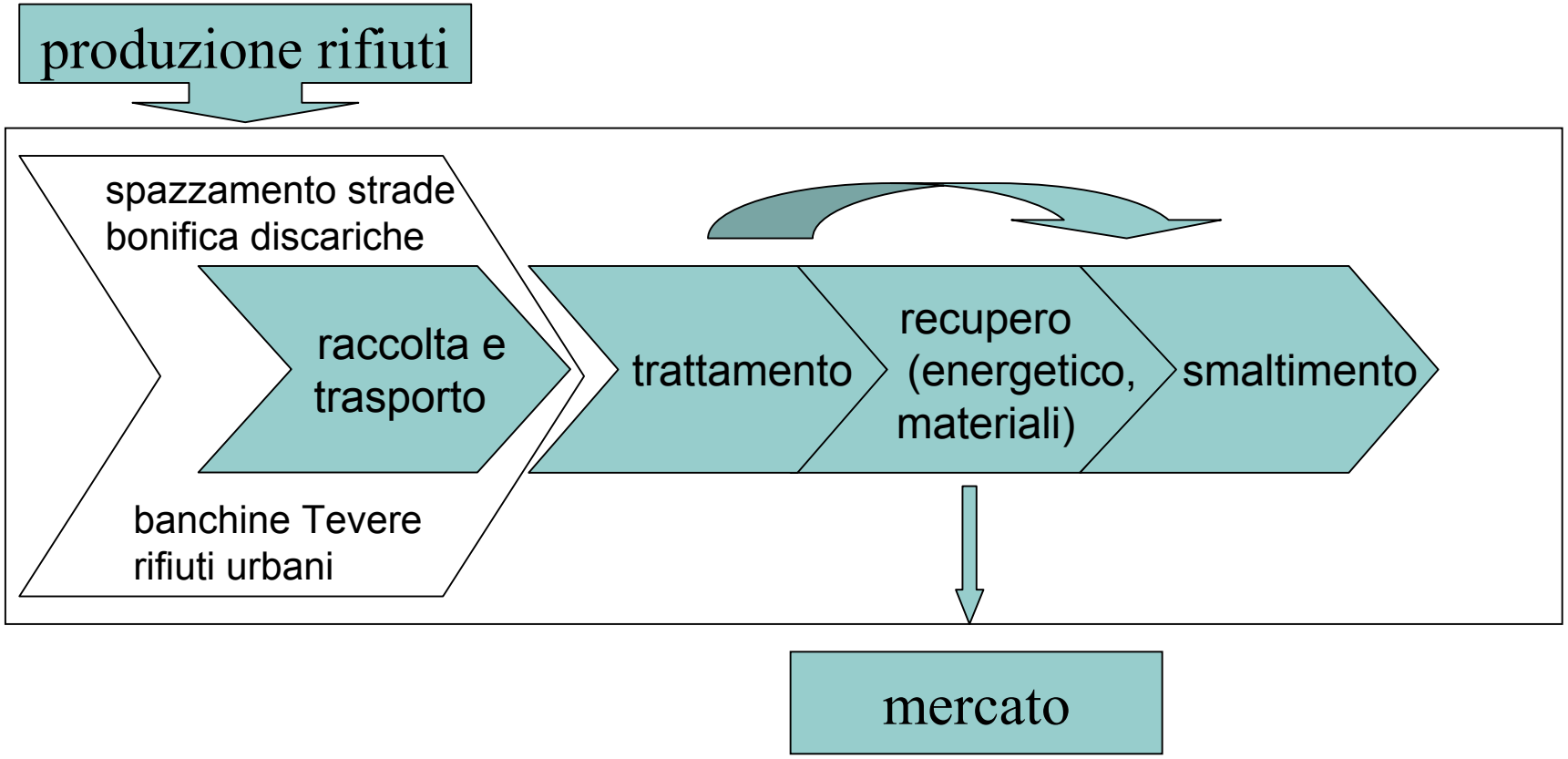


- raccolta, trasporto, trattamento, recupero rifiuti urbani, urbani pericolosi e assimilati agli urbani
- pulizia strade
- servizi funebri
- servizi a pagamento: incenerimento rifiuti speciali ospedalieri

AMA S.p.A. : alcuni dati

- 3 milioni di abitanti serviti a Roma
- 1.600.000 t/anno di rifiuti raccolti e smaltiti
- 100.000 contenitori sul territorio
- 2074 automezzi
- 95 sedi
- 6400 dipendenti
- oltre 3 milioni di abitanti serviti worldwide

Core Business: il Ciclo dei Rifiuti



La sicurezza nelle Public Utility: il caso AMA

sistemi	***tempi di risposta***
trasporti	secondi
elettrici	secondi
telefonici	secondi
idrici	minuti
igiene urbana	ore

1985	AMNU
1989	Divisione SI
1994	Piano sicurezza
1999	Piano prog. sicurezza
1999	Conformità Y2k
2000	Doc. programmatico
2003	Blackout energetico

Normativa, vincoli contrattuali, adempimenti AMA

- Decreto Legislativo n.196 del 30 giugno 2003 (nuovo TU sulla privacy) che sostituisce la Legge 675/96 e il DPR 318/99
- Contratto di servizio
- Carta dei servizi
- Authority
- Piano Progetto Sicurezza Informatica
- Organizzazione Sicurezza Informatica
- Documento programmatico sulla sicurezza: misure minime

Legame tra TU 126/2003 & Crisis Management

- La **normativa**, attraverso il *Documento Programmatico* ripreso dal TU 126/2003 richiede un'analisi conoscitiva dell'azienda, l'identificazione dei data asset, l'analisi e la gestione del rischio (contromisure di sicurezza fisiche e logiche) con riferimento ai dati personali, sensibili, giudiziari

Legame tra TU 126/2003 & Crisis Management

- La ***conoscenza del business*** consente di assegnare le priorità in funzione della gravità del disservizio e della minaccia alla sopravvivenza dell'azienda (o, nel caso delle Public Utility, del top management)

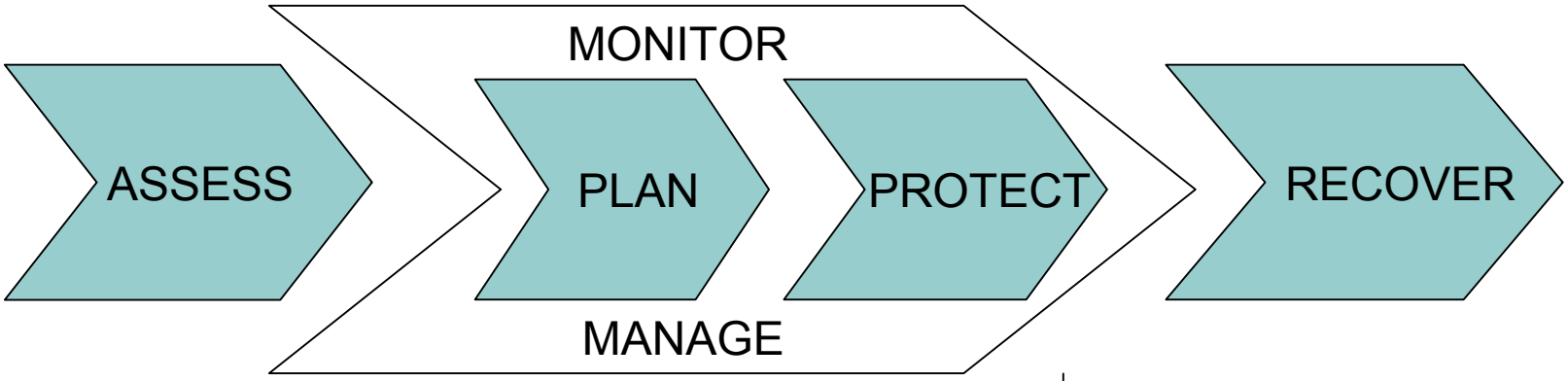
AMA:
Piano Progetto Sicurezza (1999)

- Sicurezza: identificazione e controllo accessi
- Integrità dei dati: Backup/Restore centralizzato
- Network management: livello di servizio e disponibilità dei sistemi

AMA: Documento Programmatico sulla Sicurezza (2000)

- Standard di sicurezza fisica dei sistemi ed accesso alle aree di calcolo
- Criteri di integrità dei dati sensibili e modalità di accesso agli stessi
- Definizione dei criteri di sicurezza sulle reti
- Eventi anomali
- Piano di formazione
- Procedure di audit

La catena della sicurezza ICT:



Analisi del Rischio
Business Impact Analysis
Lista minacce
Analisi vulnerabilità
Esame asset

Gestione del rischio (I)
Contromisure
Security Policy Plan
Disaster Recovery
Security Audit

Gestione del rischio (II)
Incident Response
Business Continuity
Business Restoration

Aziende di Igiene Urbana: principali fattori di vulnerabilità

Dall'esterno
Blackout elettrico
Approv.to idrico
Sciopero distrib.ri carburante
Sciopero trasporti
Virus informatici
Acts of God

Dall'interno: blocco sistema
Informativo Sedi Periferiche
Telefonico
Integrato degli Stabilimenti
Sportello e telesportello
TC impianto di incenerimento
Gestione Conferimenti
LAN e Network Management

Valutazione dei rischi (metodologia Gartner)

Livello	*Descrizione*	*Esemplificazione*
0	nessun rischio	funzionamento normale
1	inconvenienti minori	completa disponibilità delle funzioni aziendali
2	inconvenienti di tipo limitato	parziale indisponibilità
3	blocco di alcune unità organizzative	blocco di alcune attività
4	blocco di alcune unità operative	blocco di alcuni processi
5	effetti catastrofici	lunga sospensione serv.

AMA: WBS di sistemi e applicazioni

Dominio	*Esemplificazione*
Infrastrutture informatiche	Call center, help desk, TLC, LAN, IVR Internet/Intranet, mainframe, server
Applicazioni & procedure	Gestione interna, esterna, per il cittadino
Sistemi di controllo e processo	Sistemi di pesatura, robot, rilevatori presenze, PLC
Impianti tecnici e infrastrutture	Allarme, antincendio, condizionamento elettrico, radio, ascensori,illuminazione
Fornitori e business partner	Materiali, ricambi, carburante
Servizi	Gestione interna per il cittadino

AMA: matrice dei rischi

	Energia	*Acqua*	*Tel. Fix*	*Tel. Mobile*	*Radio*	*ICT*	*HW embedded*	*Fornitori*
sala operativa	X		X	X	X	X		
autorimesse	X	X	X	X	X	X		X
officine	X		X	X	X	X		X
unità perif.	X	X	X	X	X	X		X
unità P.I.	X	X	X	X	X			X
mezzi					X		X	X
pese	X			X			X	X
forno	X	X		X		X	X	X
sist. sicurezza	X						X	
ascensori	X						X	X

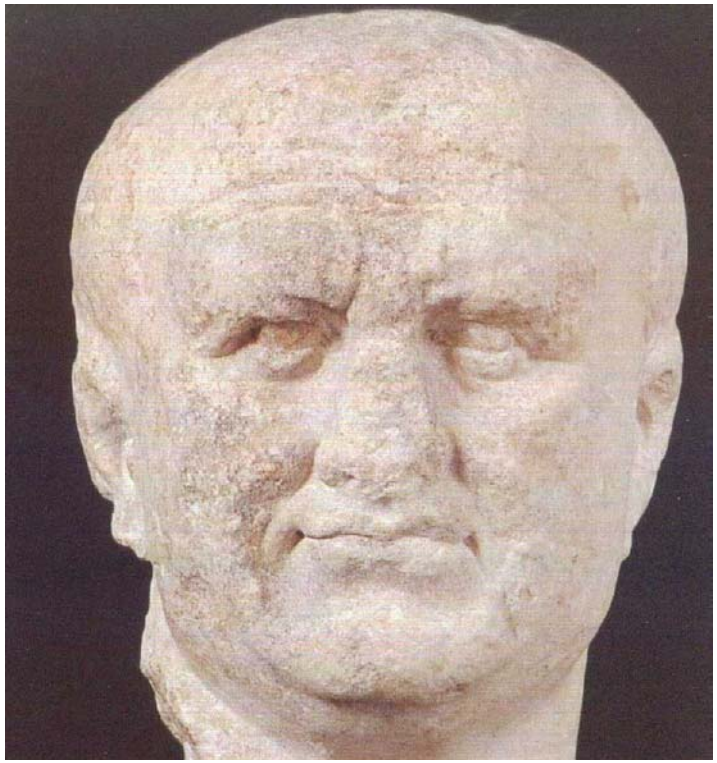
Contromisure

- **fisiche**: controllo dell'accesso fisico, firewall, UPS, ridondanza dell'hardware e dei dati (sistemi RAID)
- **logiche**: amministrazione e controllo degli accessi
- **organizzative**: turni di reperibilità e controllo remoto (home console, messaggistica su telefonia mobile)
- **procedurali**: salvataggi dei dati (backup&restore), contratti di assistenza

Blackout elettrico 28 settembre 2003

- I sistemi informatici si sono disattivati regolarmente e sono ripartiti non appena è tornata la corrente
- Il sistema radio ha continuato a funzionare
- AMA ha fornito per prima al Campidoglio un gruppo di continuità

Conclusioni



La normativa sulla privacy, che entra in vigore dal 1 gennaio 2004, costituisce un'opportunità per approntare un sistema di *Business Continuity & Crisis Management* con investimenti addizionali contenuti