



Centro Tecnico
Presidenza del Consiglio dei Ministri

La Rete Unitaria delle P.A.: *Organizzazione e Gestione della Sicurezza*

Massimiliano Pucciarelli

segreteria tecnica direzione

m.pucciarelli@ct.rupa.it
puma@acm.org

Corso Sicurezza Reti – Università di Salerno

Salerno, 8 aprile 2002



RUPA: Organizzazione e Gestione Sicurezza

AGENDA

- ❖ Origini della RUPA
- ❖ Quadro contrattuale
- ❖ Modello architetturale
- ❖ Requisiti di Sicurezza
- ❖ Sistema di Gestione della Sicurezza
- ❖ Soluzioni tecnologiche e servizi di sicurezza
- ❖ Audit di Sicurezza
- ❖ Risultati del primo Audit di Sicurezza

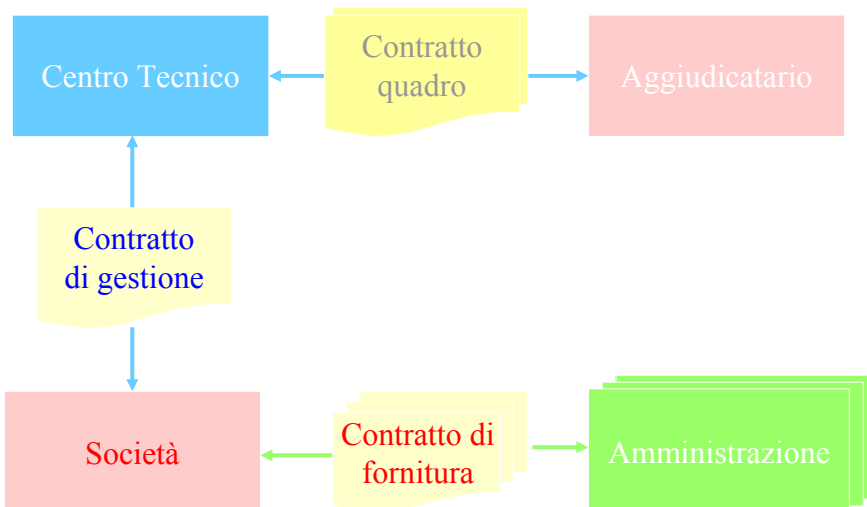


RUPA - Le tappe fondamentali

- 5/9/95: Direttiva del Presidente del Consiglio linee per realizzazione Rete Unitaria
- 10/9/95 - 31/1/96: studio di fattibilità
- 5/2/98: bando di gara
- 28/12/98: aggiudicazione del lotto n°1 alla società Telecom Italia
- 11/2/99: aggiudicazione del lotto n°2 alla società EDS
- 01/03/99: completa operatività Centro Tecnico RUPA
- 31/5/99: sottoscrizione contratto quadro trasporto
- 23/6/99: sottoscrizione contratto quadro interoperabilità
- 6/10/99: sottoscrizione contratto di gestione dell'interoperabilità



RUPA: Quadro contrattuale



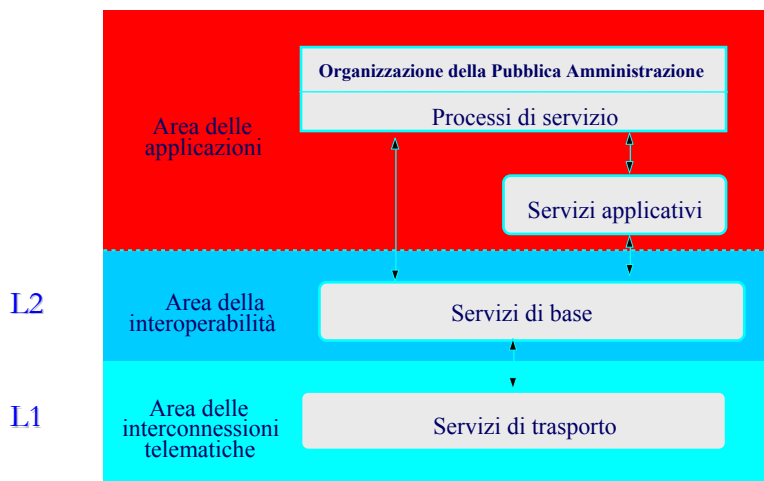


RUPA: ... chi stipula cosa

- **Il Centro Tecnico ha stipulato due *contratti quadro*:**
 - uno con l'Aggiudicatario dei Servizi trasmissivi di Trasporto,
 - uno con l'Aggiudicatario dei Servizi per l'Interoperabilità;**ed un *contratto di gestione* con la Società costituita dall'Aggiudicatario dei Servizi per l'Interoperabilità.**
- **Ogni Amministrazione stipula due *contratti di fornitura*:**
 - uno con la Società costituita dall'Aggiudicatario dei Servizi trasmissivi di Trasporto;
 - uno con la Società costituita dall'Aggiudicatario dei Servizi per l'Interoperabilità.
- **Ogni Contratto-quadro è parte integrante dei relativi contratti di fornitura, per l'interoperabilità anche del contratto di gestione.**

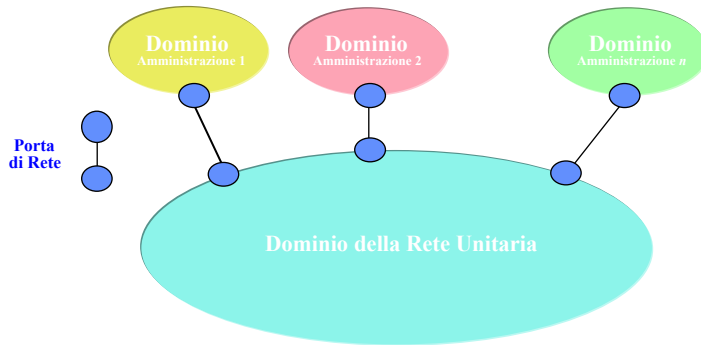


RUPA: aree di intervento

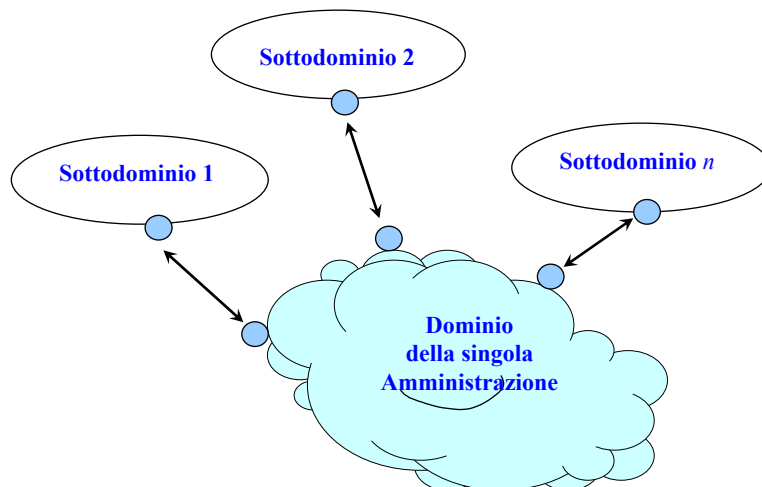




RUPA: il modello architetturale

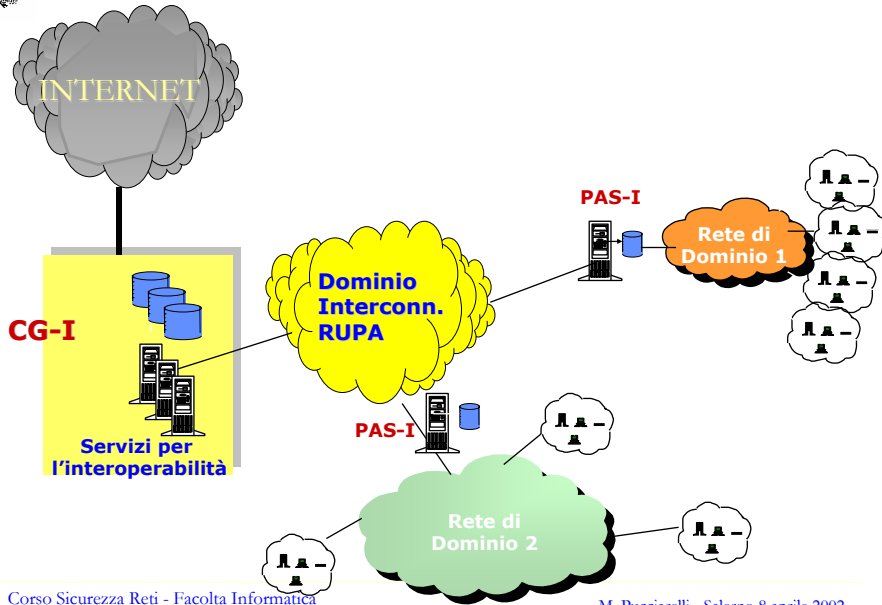


RUPA: struttura interna dei domini della PAC

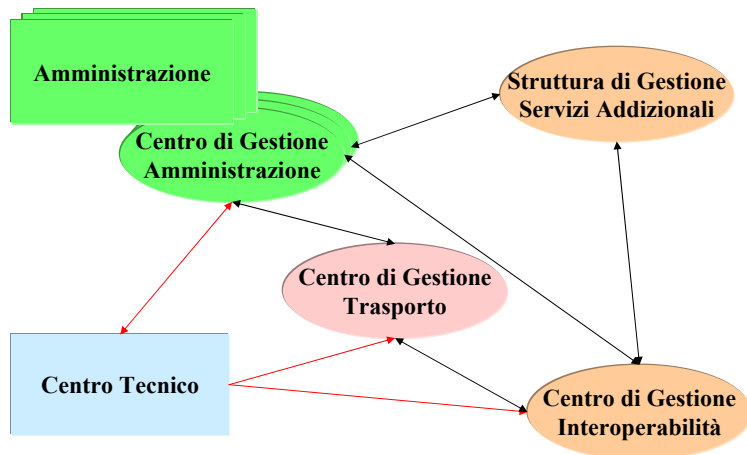




RUPA: architettura di massima



RUPA: organizzazione per la gestione





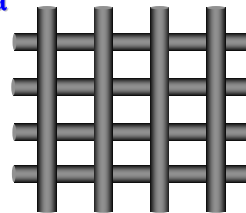
RUPA: il Centro Tecnico

- Coordina l'attività di erogazione dei servizi tra Amministrazioni.
- Fornisce i locali per il Centro di Gestione per l'Interoperabilità.
- Vigila sulla qualità dei servizi e sull'attuazione delle misure di sicurezza.
- Pianifica l'evoluzione dei servizi.
- Assiste le Amministrazioni sotto il profilo tecnico, e nella stipula e gestione dei singoli contratti di fornitura.
- Supporta le procedure di Revisione Generale previste dai contratti, in particolare quella di aggiornamento dei prezzi.



RUPA: Requisiti di Sicurezza

- Analisi del rischio
- Amministrazione della sicurezza
- Audit
- Test ciclici di impenetrabilità
- Test discrezionali di impenetrabilità
- Verifiche architettura
- Incidenti di sicurezza
- Allarmi e interventi
- Controllo e analisi dei log
- Norme per il personale che opera nei Centri di Gestione dei fornitori





Il Bando di Gara RUPA: requisiti

“Il Fornitore dovrà garantire la sicurezza dei servizi erogati”

- **Sicurezza Fisica**
 - accesso controllato alle aree contenenti apparecchiature critiche
 - protezione contro eventi accidentali (incendio, allagamento, ...)
- **Sicurezza Logica**
 - sistemi operativi e software di base
 - regole per le password
 - amministratori di sistema, di sicurezza, di auditing
 - controllo e analisi dei log
 - attacchi sistematici



RUPA: Protezione degli apparati di Rete

- **Protezioni fisiche**
 - Apparati di rete in locali controllati
 - Edifici con tutte le porte d'ingresso ad accesso controllato
 - Sensori anti-permanenza
 - Sensori anti-incendio anti-allagamento
- **Protezioni logiche**
 - Profili di accesso differenziati
 - Accesso agli apparati (network management) con user-id e password solo da CG-T
 - Sistemi “one-time-password” per i router del CG-T e per i router che implementano il protocollo IPSEC
 - ACL sui router di accesso
 - Correlazione eventi



RUPA: Protezione sistemi di gestione della Rete

- Protezioni fisiche del CG
- Controllo dell'accesso fisico al CG
- Autenticazione mediante "one-time-password" per l'accesso ai sistemi del CG da parte degli operatori
- Segmentazione e protezione della LAN del CG mediante firewall
- Sistemi di rilevamento degli attacchi in tempo reale
- Sistemi antivirus
- Sistemi di controllo dell'integrità dei file (log)

CG= Centro di Gestione del fornitore



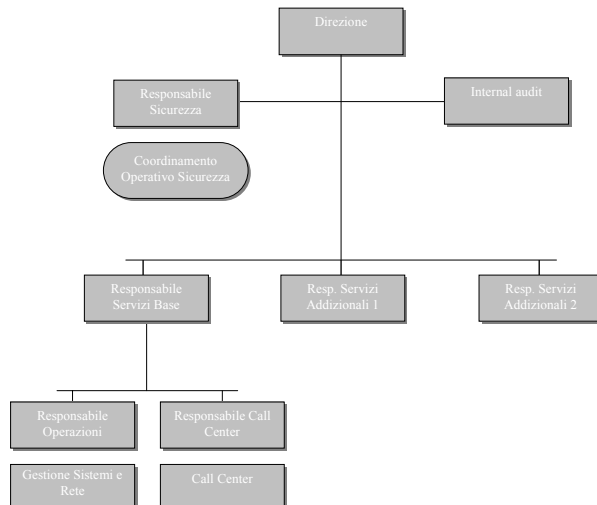
Il Bando di Gara RUPA: requisiti

“Il Fornitore dovrà garantire la sicurezza dei servizi erogati”

- Definizione nell'organizzazione di una **struttura dedicata** alla sicurezza
- Individuazione del **“Responsabile della Sicurezza”**
- Definizione di specifiche **Procedure** per garantire che le specifiche di sicurezza siano rispettate



RUPA: Organizzazione della sicurezza

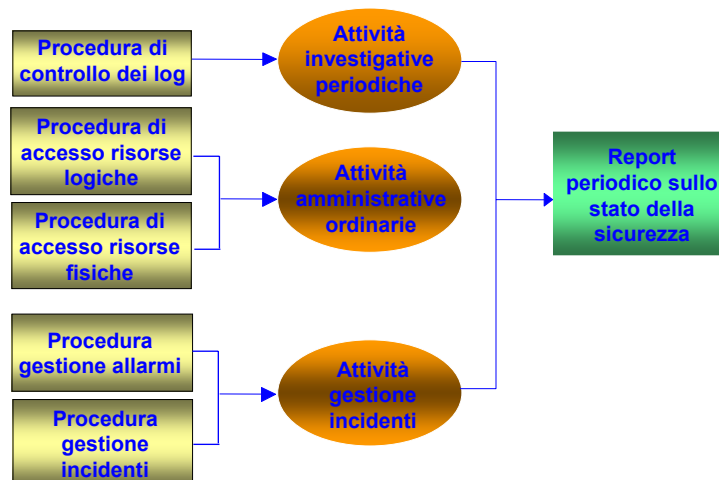


Corso Sicurezza Reti - Facoltà Informatica

M. Pucciarelli - Salerno 8 aprile 2002



RUPA: Esercizio dispositivi di sicurezza

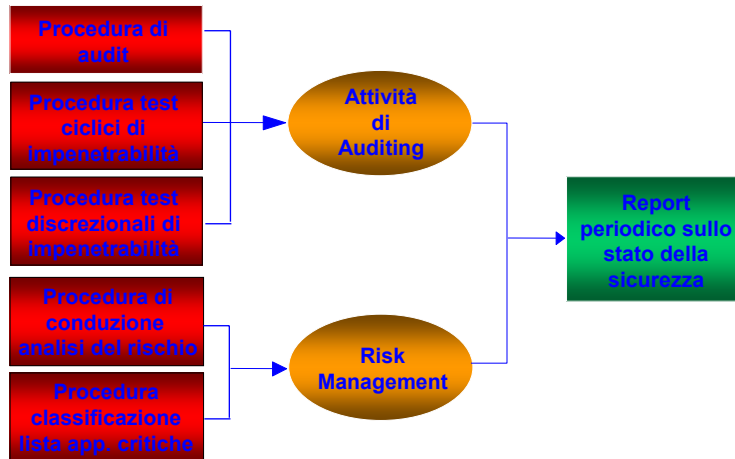


Corso Sicurezza Reti - Facoltà Informatica

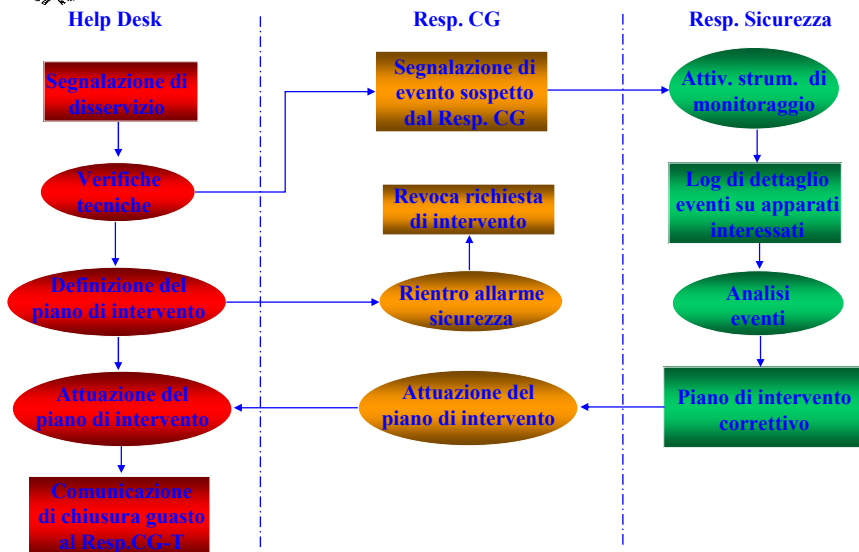
M. Pucciarelli - Salerno 8 aprile 2002



RUPA: Verifiche di Sicurezza

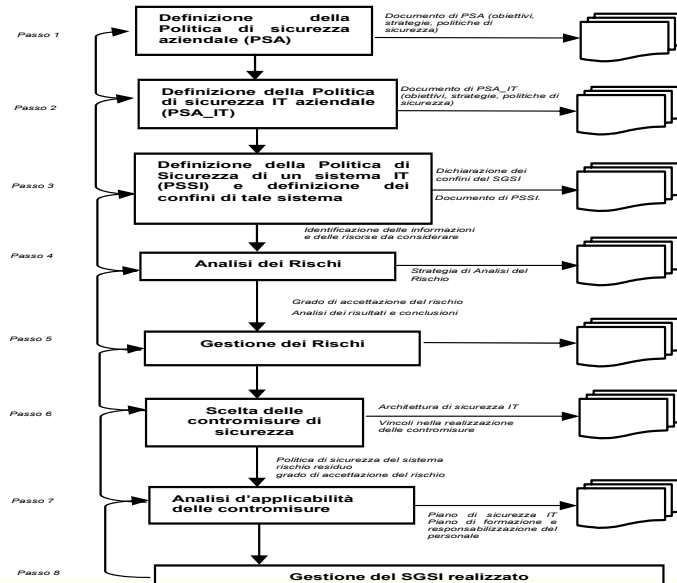


RUPA: Correlazione eventi





RUPA: Organizzazione e Gestione Sicurezza



RUPA: definizione di una PSA

- OBIETTIVI di sicurezza** ➡ Cosa l'azienda si propone di ottenere in termini di sicurezza, ossia qual è il livello di rischio che può essere tollerato
- STRATEGIE di sicurezza** ➡ Come l'azienda si propone di raggiungere gli obiettivi di sicurezza fissati.
- POLITICHE di sicurezza** ➡ Quali sono le regole aziendali da rispettare per raggiungere gli obiettivi di sicurezza fissati.

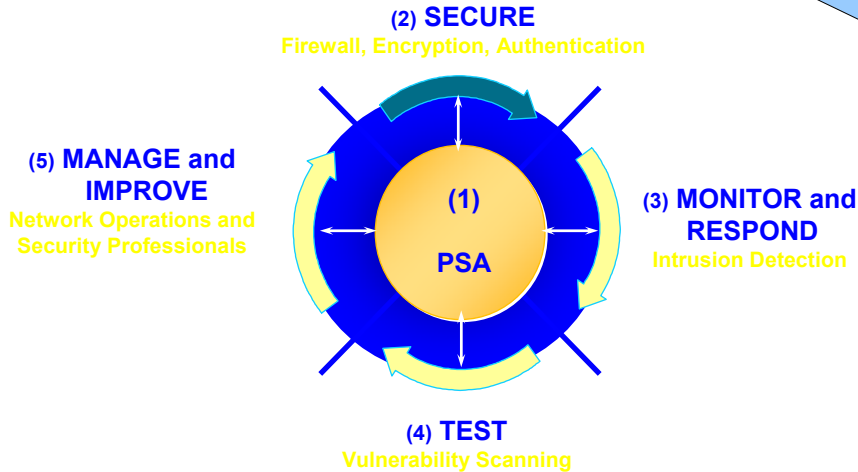
PSA: Politica di Sicurezza Aziendale



RUPA: la sicurezza ...

... tenuto conto che ...

...esiste il "Processo della Sicurezza"



RUPA

Tenuto conto che ...

Requisiti Sicurezza IT:

- **Integrità.**
 - L'informazione alterata deve essere rilevabile.
- **Disponibilità.**
 - L'informazione deve essere accessibile a utenti e processi autorizzati.
- **Confidenzialità.**
 - L'informazione deve essere nota solo a chi ne ha diritto.
- E con riferimento a sistemi connessi in rete:
 - **Autenticazione.**
 - Certezza dell'identità del mittente da parte del destinatario.
 - **Non ripudio.**
 - I soggetti coinvolti in uno scambio di informazioni non possono negare l'invio di tali informazioni.



RUPA: Obiettivi di sicurezza

Durante l'erogazione dei servizi alle Amministrazioni, il fornitore persegue i seguenti obiettivi fondamentali di sicurezza:

- Garantire riservatezza ed integrità delle informazioni gestite ed in transito
- Impedire a terzi di accedere o modificare dati e risorse di pertinenza delle Amministrazioni
- Impedire a personale interno e delle Amministrazioni di accedere o modificare dati e risorse senza averne autorizzazione
- Indirizzare al corretto destinatario le informazioni gestite



RUPA: Principi di sicurezza *(Strategie e Politiche)*

- Il Fornitore è garante della sicurezza dei servizi erogati
- Il Fornitore si impegna a mantenere aggiornato il sistema di sicurezza rispetto ai più elevati standard di mercato
- Le risorse interne dei CG possono essere usate per i soli scopi istituzionali
- Regole, autorizzazioni, privilegi e diritti di accesso a risorse, dati e servizi sono basati sul principio della *“minima conoscenza”*
- La configurazione dei sistemi di sicurezza è basata sul principio che *“tutto ciò che non è espressamente autorizzato è proibito”*
- Tutti gli apparati di sicurezza sono realizzati e gestiti secondo identici criteri e modalità gestionali



RUPA: Metodologia di analisi del rischio

Identificazione di:

- **ASSET**
- **OBIETTIVI**
- **MINACCE**

Tre modelli di calcolo:

- Rischio su parametri BS-7799
- Rischio su parametri tecnologici
- Efficacia delle barriere su modello topologico



Analisi del rischio

Esecuzione dell'analisi del rischio:

- In fase di progettazione
- Su base annua
- In seguito a gravi incidenti di sicurezza

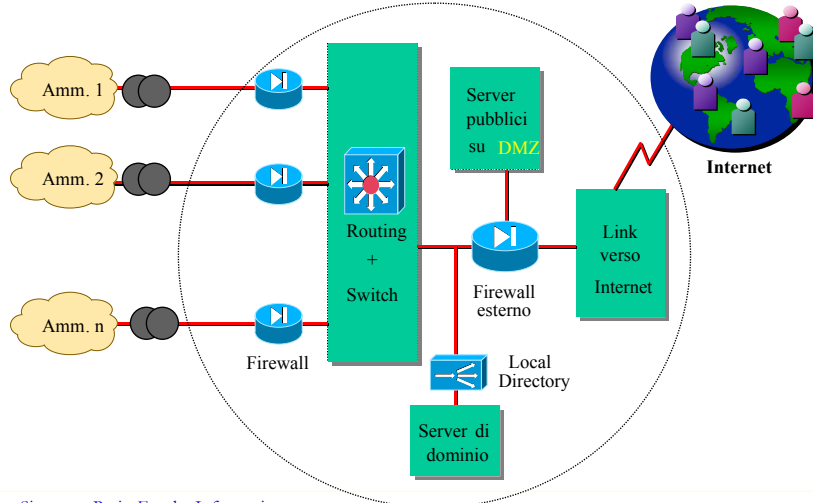
Risultati all'avvio del progetto:

- Riduzione globale del rischio superiore al 92%



RUPA: architettura del CG-I

Risultati dell'applicazione della RA



RUPA: la verifica del SGSI

Per **Audit di Sicurezza** si intende

“un’attività di verifica che accerta il raggiungimento degli obiettivi definiti nella politica di sicurezza dato l’insieme delle misure organizzative, procedurali e tecnologiche adottate dal fornitore”



RUPA: Audit di Sicurezza

Obiettivi

- Effettuare una verifica completa del sistema di gestione della sicurezza
- Individuare carenze e criticità non conformi con quanto stabilito dal capitolato e dagli obiettivi di sicurezza
- Definire e pianificare una serie di azioni specifiche, basate sui risultati delle verifiche, che siano in grado di far raggiungere gli obiettivi di sicurezza prefissati. (Piano di rientro)
- Attivare il miglioramento del processo di gestione della sicurezza.



RUPA: Audit di Sicurezza

Contesto di riferimento

- Organizzazione della sicurezza
- Definizione della politica di sicurezza
- Identificazione delle misure di tipo tecnologico
- Realizzazione delle misure di tipo fisico
- Generazione e configurazione del sistema
- Procedure per la gestione del sistema e del personale

- Capitolato RUPA
- Contratto Quadro



RUPA: Audit di Sicurezza

verifica che:

- Esista un'organizzazione di sicurezza (definita nei ruoli e nei compiti)
- Esista la definizione della politica di sicurezza (obiettivi, definizione dei beni da proteggere, le modalità di accesso ad informazioni e risorse)
- La politica di sicurezza sia nota al personale
- La politica di sicurezza sia realizzata nelle misure tecniche e procedurali
- Esista la definizione delle funzioni di sicurezza logica realizzate nel sistema



RUPA: Audit di Sicurezza

verifica che

- Esista la corretta configurazione (di sicurezza) del sistema
- Esista la documentazione delle procedure di sicurezza
- Le misure di tipo fisico siano implementate
- Le procedure definite per la sicurezza costituiscano un effettivo supporto alle misure tecnologiche
- Le procedure siano note ai rappresentanti dei vari ruoli e siano applicate



RUPA: Audit di Sicurezza

Fasi principali:

- Fase 1: raccolta documentazione
- Fase 2: verifica della documentazione
- Fase 3: definizione del piano di Audit
- Fase 4: definizione test di intrusione
- Fase 5: visita sul campo
- Fase 6: esecuzione test di intrusione
- Fase 7: redazione rapporto finale

- Follow-up: continuità ed efficacia delle azioni correttive



RUPA: il primo Audit di Sicurezza periodo 2000-2001

Obiettivi :

- Verifica del rispetto della norme (BS7799)
- Verifica del rispetto delle procedure RUPA
- Verifica della consistenza delle misure di sicurezza adottate



RUPA: il primo Audit di Sicurezza

Attività :

- Audit Procedurale
- Interviste al Personale
- Verifica Nodi Esterni al CG-T
(Centrali Telecom)
- Verifica Nodi di Rete delle Amministrazioni
- Test di Penetrazione



RUPA: il primo Audit di Sicurezza

Risultati :

- Rispetto delle norme BS7799
 - 11 non conformità
- Controllo Procedure Interne
 - 7 non conformità

Su un totale di 335 CONTROLLI effettuati!



... Spazio ai quesiti !



• Copyright

- Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.
- Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà del Centro Tecnico e degli autori indicati.
- Le trasparenze possono essere riprodotte liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.
- Ogni altro utilizzo o riproduzione (ivi incluse, ma non limitatamente a, riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in completamente o in parte è vietata, se non esplicitamente autorizzata per iscritto da parte dell'autore.
- L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di sistemi e/o prodotti, ecc.
- L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. L'autore non assume alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente alla correttezza, completezza, applicabilità ed aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.