



# **LA SICUREZZA COME FATTORE CRITICO DI COMPETITIVITA' DELLE PICCOLE E MEDIE IMPRESE**

Erminio Seveso

[www.apsed.org](http://www.apsed.org)

SMAU - 20 ottobre 2005

# CHI E' L'AUSED



- **AUSED nasce nel 1976.**
- **AUSED, è una Associazione di Utilizzatori di Sistemi E tecnologie Dell'informazione , indipendente e senza scopi di lucro.**
- **AUSED si finanzia con la quota associativa**

# SCOPI DELL'AUSED



- Favorire lo scambio di esperienze tra le aziende associate.
- Promuovere il confronto su modelli organizzativi e soluzioni informatiche innovative.
- Contribuire alla valorizzazione e alla crescita della cultura informatica del Paese

# LE ATTIVITA'

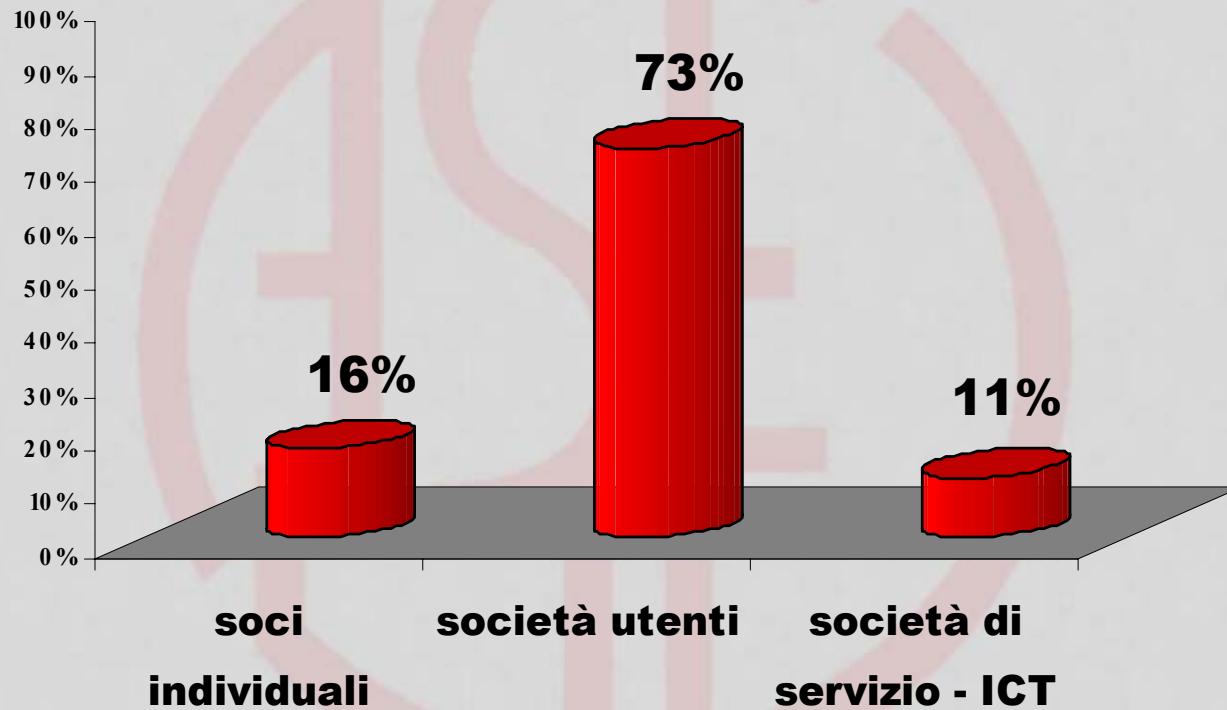
- Seminari e workshop
- Convegni
- Ricerche e indagini su temi segnalati dagli Associati
- Il “telefono amico”
- Forum sul sito Aused



# I GRUPPI DI LAVORO

- FARMA (Aziende farmaceutiche)
- GUPS (Gruppo Utenti SAP)
  
- TELECOMUNICAZIONI
- Osservatorio SICUREZZA
- BENCHMARKING
- OPEN SOURCE.

# IL PROFILO DEI SOCI



SMAU - 20 ottobre 2005

# L'OSSERVATORIO SICUREZZA



## **Costituito il 19-9-02 con i seguenti obiettivi:**

- Elaborazione di linee guida normative per la sicurezza informatica rivolte agli associati e di stimolo per le pubbliche autorità, anche in vista di certificazioni riconosciute;
- Attività di sensibilizzazione delle direzioni aziendali e di incremento della cultura aziendale sulla sicurezza informatica;
- Indagini sulla situazione della sicurezza e della valutazione dei rischi tra gli associati
- Incontri divulgativi

# ALCUNE ATTIVITA' DELL'O.S.



- Workshop dell'Osservatorio
- Classificazione dei requisiti della norma BS7799
  - *un approccio più razionale alla sicurezza*
- Manuale del Sistema Sicurezza
  - *una guida per la realizzazione delle Politiche per la sicurezza*
- Facsimile del Documento Programmatico sulla Sicurezza
  - *un supporto per realizzare il DPS*
- Indagine sugli standard della sicurezza
- Questionario di autovalutazione
- Benchmarking sulla sicurezza informatica
- Metodologia per l'Analisi dei rischi

esempi

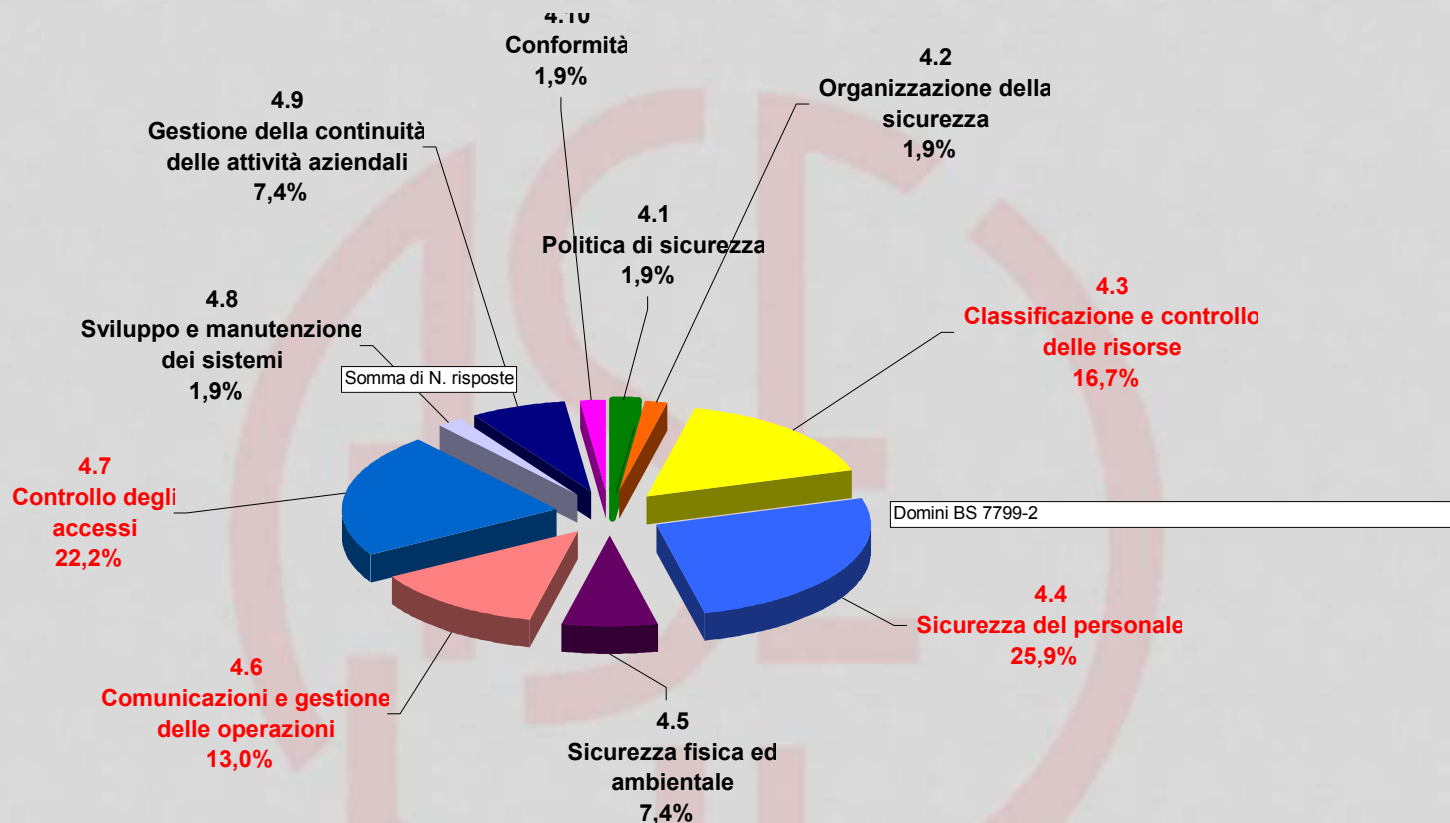


# BENCHMARKING



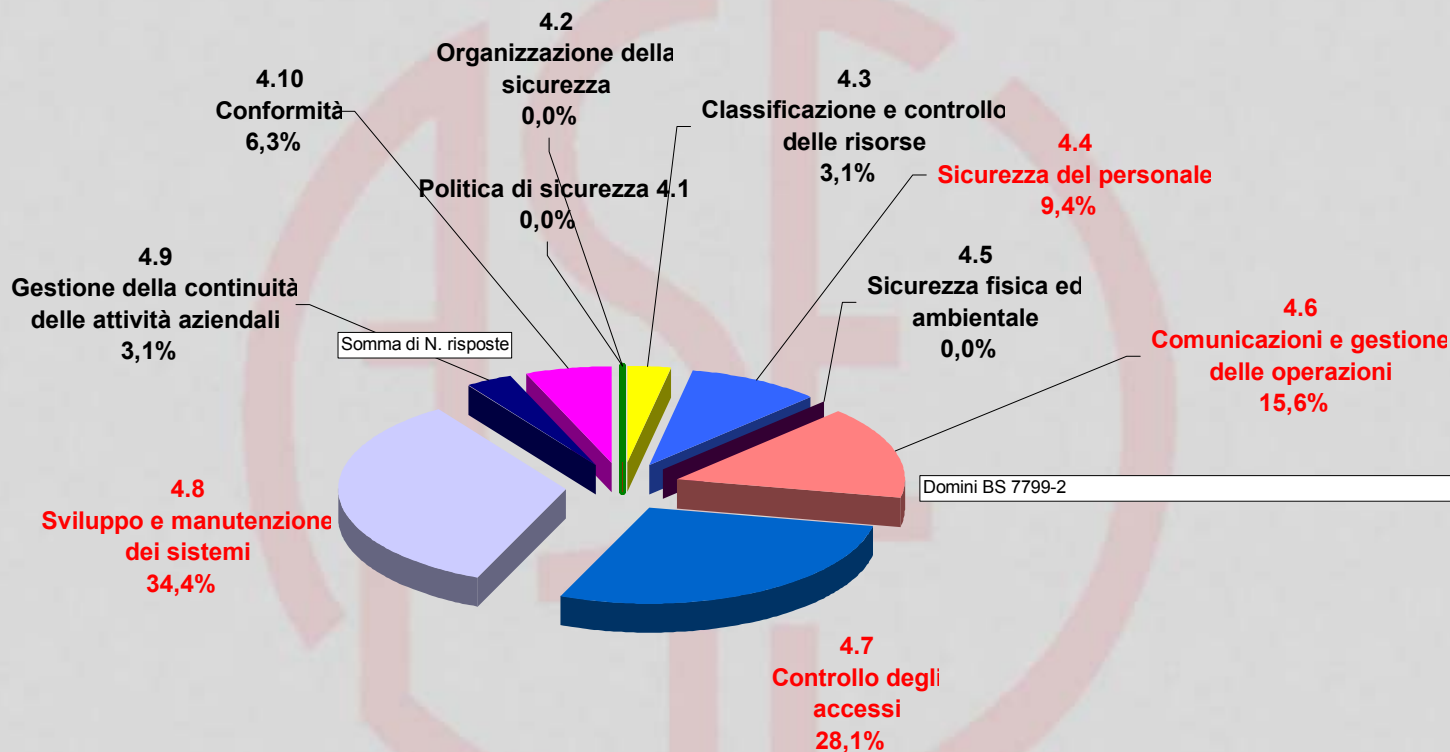
- Quali sono le maggiori **minacce** alla sicurezza delle informazioni presso la tua azienda?
- Quali sono i problemi di sicurezza delle informazioni che assorbono le **maggiori risorse** in termini di tempo al tuo staff?
- Quali sono le **azioni** che hai messo in atto per reagire con efficacia ad eventi di violazione della sicurezza delle informazioni?

# BENCHMARKING - MINACCE



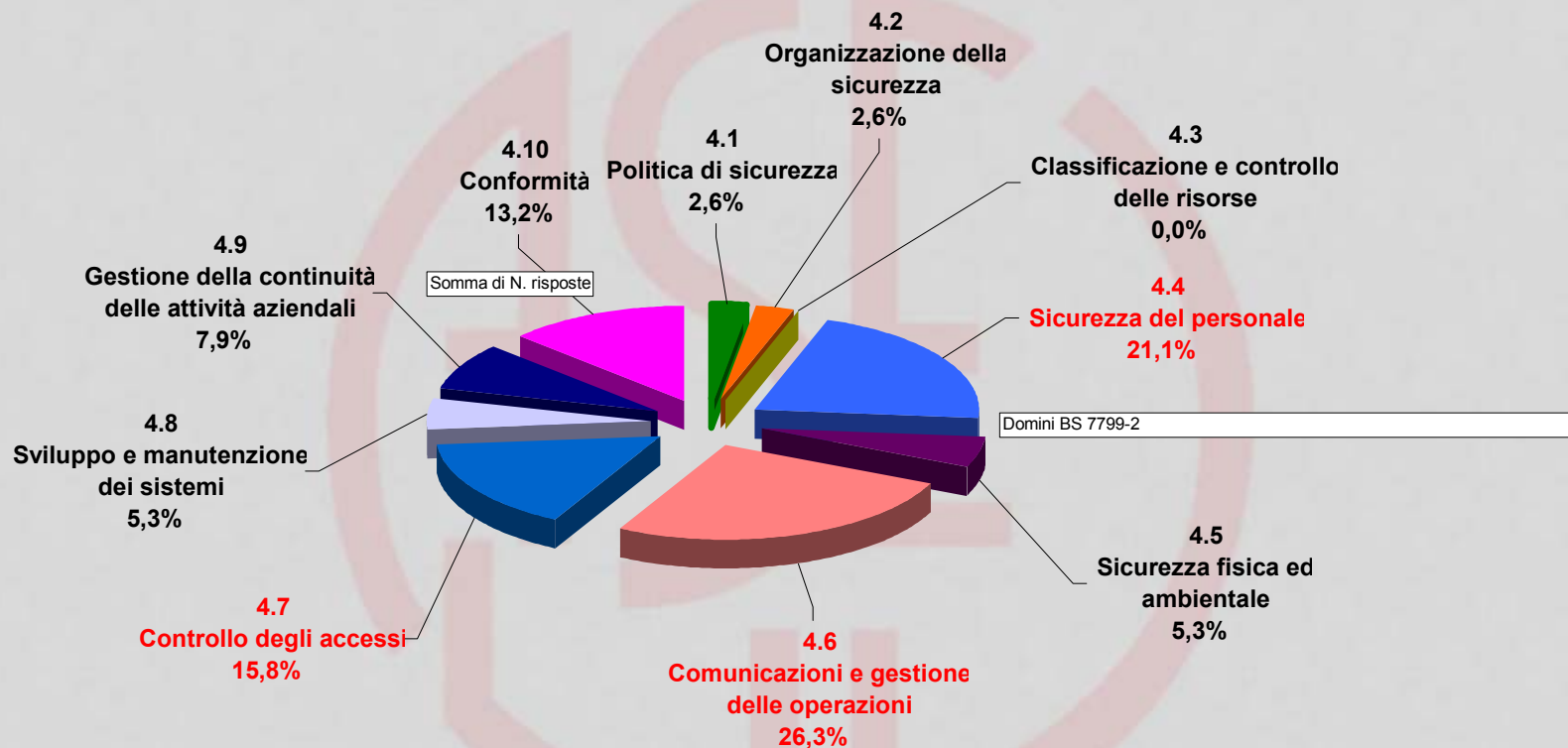
- **26%** Cultura / Formazione del Personale
- **22%** Controllo Accessi
- **17%** Controllo Risorse (HW - SW - Organizzative)
- **13%** Comunicazioni e Gestione operativa

# BENCHMARKING - RISORSE



- Il 34,4% degli sforzi sono focalizzati sulla **manutenzione dei Sistemi** che era stata definita una minaccia non rilevante (1,8%) → **Remediation**
- Gli altri segnali forti sono coerenti con le minacce → **cultura / controllo**

# BENCHMARKING – AZIONI



**26,3% INTERVENTI TECNOLOGICI (firewall / VPN / DMZ / antivirus / Backup ...)**

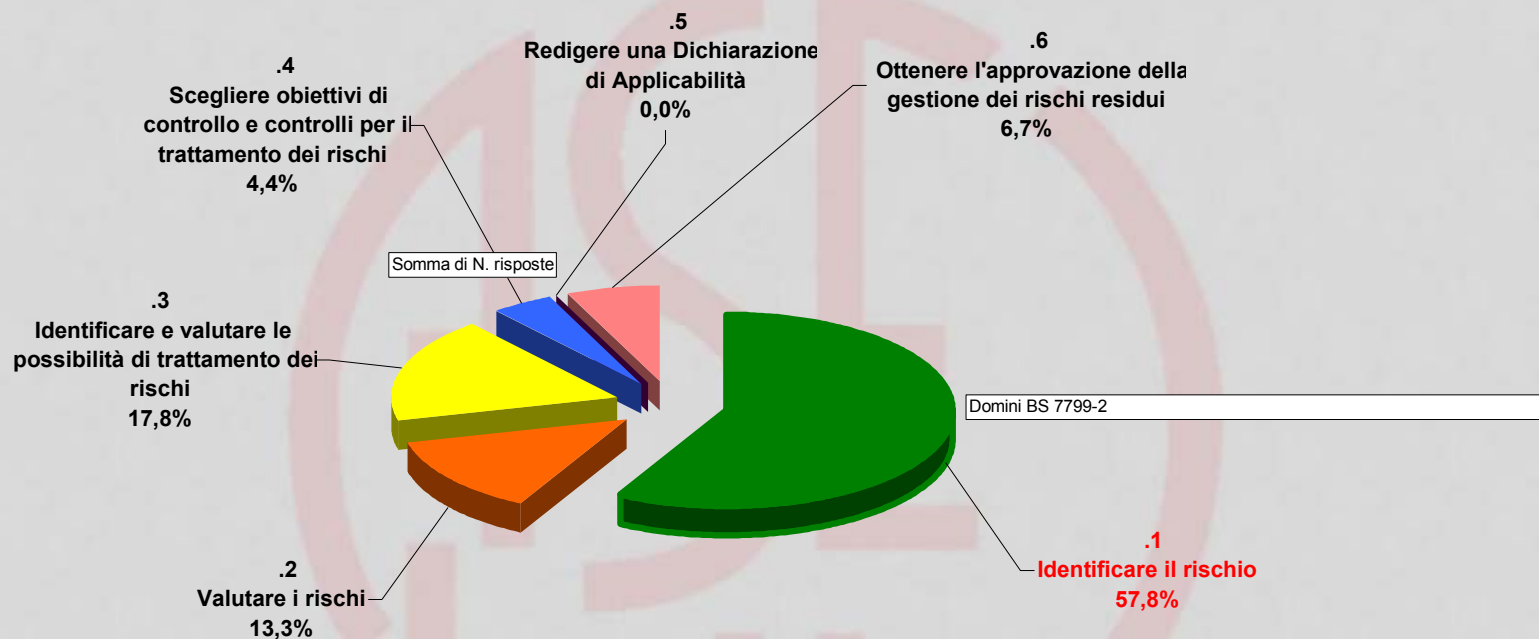
**21,1% FORMAZIONE PERSONALE**

**15,8% CONTROLLO ACCESSI**

- E' maturata la **consapevolezza** che la Sicurezza del Patrimonio Informativo è un Processo chiave per la stabilità delle Imprese → si investe
- Le PMI si sono attivate anche se ancora con soluzioni **“a macchia di leopardo”** e fundamentalmente tecnologiche
- L'esigenza di **Impresa Compliance** (196/2003, SOA, 231, Siti e-Commerce certificati, ...) sta spostando l'approccio alla Sicurezza verso una soluzione strutturata, parte integrante del Processo Informatico e di quello di Auditing,
- In questo cammino è forte l'esigenza di **Confronto, supporto, esperienze.**



# ANALISI DEI RISCHI



## Risultati Benchmarking

- Quali sono i componenti essenziali per una corretta ed efficace **Analisi dei Rischi?**
- **58% → Conoscere i Rischi!**

# ANALISI DEI RISCHI



- Obiettivo del progetto è stato fornire un prodotto semplice, di facile utilizzo e personalizzabile per l'approccio all'adozione di un processo di Analisi dei Rischi
- Il metodo suggerito vuole essere un **punto di partenza** per maturare la consapevolezza che il fine ultimo non è la sicurezza assoluta ma una equilibrata gestione del rischio in continuo mutamento
- Ad oggi sono state richieste **37** copie dello strumento da parte di Associati Aused.

# ANALISI DEI RISCHI



## **Caratteristiche della metodologia Aused**

- Semplicità
- Efficace individuazione dei beni
- Verosimili minacce incombenti
- Modalità per le rilevazioni
- Efficacia/efficienza

## **La struttura della metodologia**

- Individuazione dei componenti che costituiscono gli elementi di riferimento
- Sviluppo delle fasi di applicazione la metodologia

# ANALISI DEI RISCHI



## Individuazione dei componenti

- I beni da proteggere
- Le minacce dalle quali proteggerci
- Il questionario per individuare il livello di protezione del patrimonio informatico
- Le Azioni Correttive consigliate
- Le tipologie dei rischi per una migliore valutazione delle priorità alle Azioni Correttive
- L'analisi dei rischi

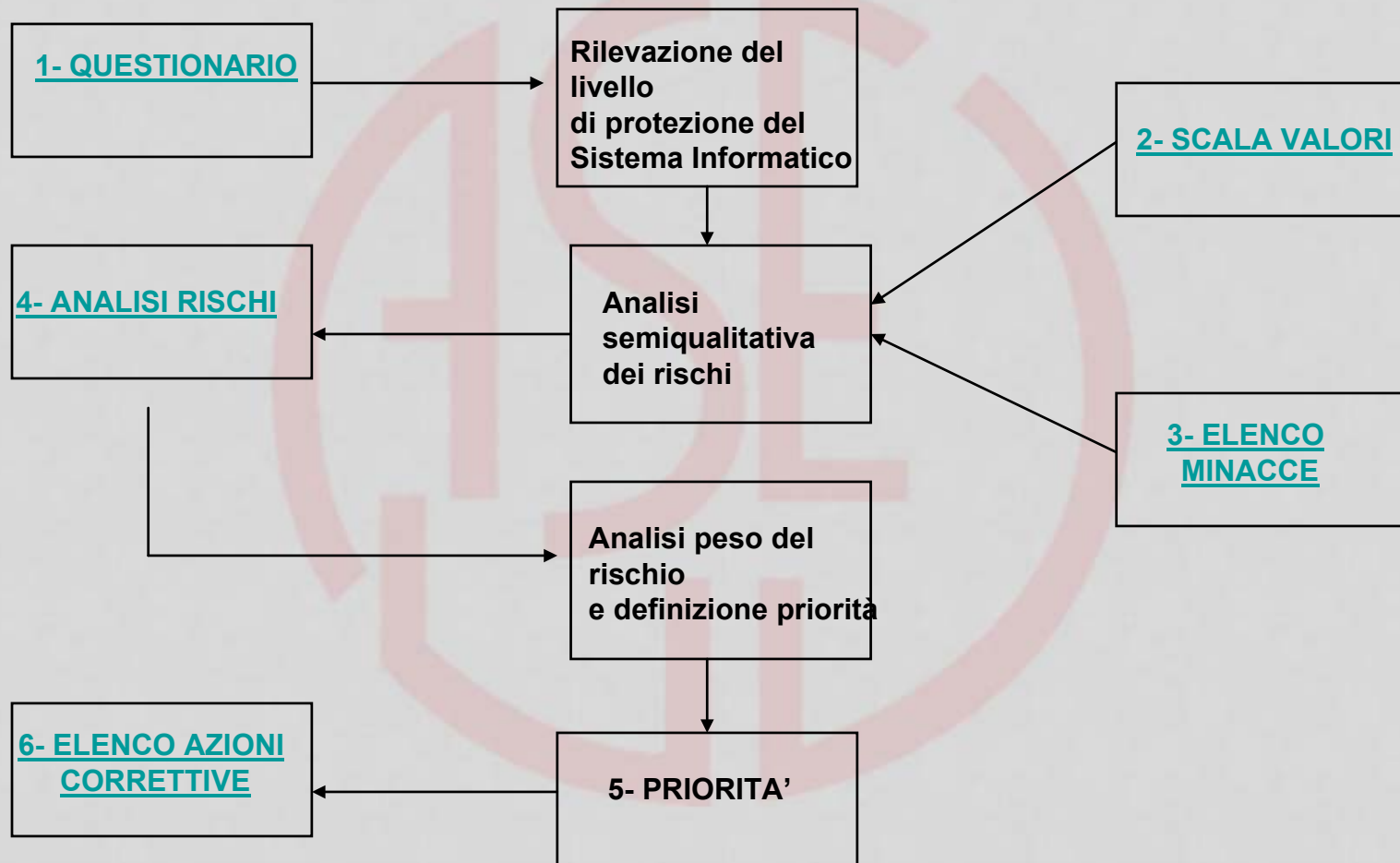
# ANALISI DEI RISCHI



## Sviluppo delle fasi

- Fase 1  
rilevazione del livello di protezione del patrimonio informatico
- Fase 2  
analisi semiquantitativa dei rischi
- Fase 3  
analisi del peso del rischio, valutazione, individuazione della Azioni Correttive e definizione delle priorità

# ANALISI DEI RISCHI





**per informazioni**

**[www.apsed.org](http://www.apsed.org)**

SMAU - 20 ottobre 2005