




ENAV *S.p.A.*

SOCIETÀ ITALIANA PER L'ASSISTENZA ALLA NAVIGAZIONE AEREA

Roma 17 giugno 2005



**Controllo e assistenza  
del traffico aereo,  
integrati nel sistema  
aeronautico europeo  
Servizio informazioni  
aeronautiche.  
Strutture operative  
comprendenti  
4 Centri nazionali di rotta,  
Roma, Milano,  
Padova e Brindisi  
e 39 aeroporti  
dislocati sul  
territorio nazionale.**

**Gestione puntuale  
e sicura, 24 ore su 24,  
di 5200 voli al giorno,  
2.000.000 ogni anno, grazie a  
s sofisticate e aggiornate  
tecnologie e a un  
personale altamente  
qualificato di 3500  
dipendenti di cui 2400  
direttamente impegnati  
nell'assistenza  
al volo.**

ITALIAN COMPANY FOR AIR NAVIGATION SERVICES



# AGENDA

- ◆ Premessa
- ◆ Sicurezza fisica
- ◆ Infrastruttura di Sicurezza
- ◆ Utilizzo delle SMART-CARD
- ◆ Tecnologia Biometrica
- ◆ Influenza del fattore umano

# PREMESSA

- ◆ **Esigenza:**
  - ◆ **Affrontare i problemi di Sicurezza nella loro globalità**
- ◆ **Soluzione:**
  - ◆ **Possibilità di differenziare l'approccio**
  - ◆ **Approccio essenziale (basato solo sulla tecnologia)**
  - ◆ **Approccio metodologico**
- ◆ **ENAV ha scelto : l'approccio metodologico**

# APPROCCIO METODOLOGICO

- ◆ Stabilire le esigenze di sicurezza
- ◆ Trasformarle in requisiti
- ◆ Implementare le soluzioni
- ◆ Verificare le rispondenza tra requisiti e soluzioni

# ANALISI DEL RISCHIO

- ◆ Individuazione dei rischi tramite i tre fattori fondamentali:
  - ◆ Minaccia
  - ◆ Vulnerabilità
  - ◆ Impatto
- ◆ focalizzata su ciascuna specifica area di valutazione
- ◆ Individuazione delle metodologie specifiche per ciascuna di esse

## ANALISI DEL RISCHIO (2)

- ◆ **Attivata una Risk Analysis:**
  - ◆ **Identificazione della Minaccia**
  - ◆ **Valutazione dell'impatto sui beni critici di ENAV**
  - ◆ **Valutazione ed Analisi delle Vulnerabilità**
    - ◆ **Attività di Penetration Testing**
    - ◆ **Attività di exploiting manuale delle Vulnerabilità**
  - ◆ **Valutazione dell'esposizione al Rischio**
  - ◆ **Identificazione le contromisure da porre in atto**

# METODOLOGIE

## Standard internazionali (ove possibile)

- ◆ Esempio:
  - ◆ BS7799 (ISO/IEC 17799 – part 1)
  - ◆ SSE-CMM (ISO/IEC 21827)
  - ◆ GMITS (ISO/IEC 13335)

# CRITERI DI VALUTAZIONE

- ◆ TCSEC (Trusted Computer System Evaluation Criteria – Orange Book)
- ◆ ITSEC (Information technology Security Evaluation Criteria
  - ◆ ITSEM
- ◆ CC (Common Criteria – ISO/IEC 15408)

# VANTAGGI NELL'USO DEGLI STANDARD

- ◆ **Certificazione**
- ◆ **Standardizzazione delle procedure**
- ◆ **Facilità di implementazione**
- ◆ **Facilità di monitoraggio e manutenzione**

# SICUREZZA FISICA

- ◆ Piano Nazionale per il controllo mediante:
- ◆ Sistemi antintrusione videosorveglianza, antiscavalcamento e recinzioni;
- ◆ Interventi su segnalazione di infrazioni con sistemi di radiosorveglianza in siti non presidiati;
- ◆ Controllo accessi basato su smart-card e controlli biometrici;

# INFRASTRUTTURA DI SICUREZZA TECNICA

- ◆ Utilizzo PKI per l'autenticazione
- ◆ Profilazione utenti
  - ◆ Strumenti di Single sign-on
  - ◆ Accesso controllato nei locali e siti
- ◆ Controlli Biometrici per accessi in aree riservate e autenticazione forte su applicazioni di rilevanza strategica

# INFRASTRUTTURA DI SICUREZZA ORGANIZZATIVA

## ◆ Normativa

- ◆ Codice in Materia di Protezione dei Dati Personali
- ◆ Normativa interna all'organizzazione

## ◆ Formazione

- ◆ Piano di Formazione di base (sicurezza) suddivisa per ruoli e responsabilità
- ◆ Piano periodico di aggiornamento
- ◆ Piano di sensibilizzazione del personale

# SERVIZI INTERNET

- ◆ Condizioni di utilizzo di Internet
- ◆ Politiche di utilizzo corretto dei servizi
- ◆ Politiche sull'utilizzo di internet e posta elettronica

# INFLUENZA DEL FATTORE UMANO

- ◆ **Identificazione della minaccia**
  - ◆ Minacce ad opera di soggetti esterni (outsiders)
  - ◆ Minacce ad opera di soggetti interni (insiders)
- ◆ **Applicabilità delle contromisure:**
  - ◆ Equilibrio tra elevato livello di sicurezza e l'impatto che eventuali contromisure hanno sul personale (risposta degli utenti)
  - ◆ Formazione continua

# contatti

**Avv. Francesco Di Maio**  
**Direttore Security**  
**[fdimaio@enav.it](mailto:fdimaio@enav.it)**

**Bruno Carbone**  
**Responsabile Sicurezza Informatica**  
**[bcarbone@enav.it](mailto:bcarbone@enav.it)**