

# La sicurezza nelle grandi organizzazioni

Arturo Salvatici

Segretario Consorzio I.B.I.S.C.O.

# Il Consorzio I.B.I.S.C.O.

Riunisce società di outsourcing che operano nel mercato bancario. È stato costituito nel 1989 con lo scopo di:

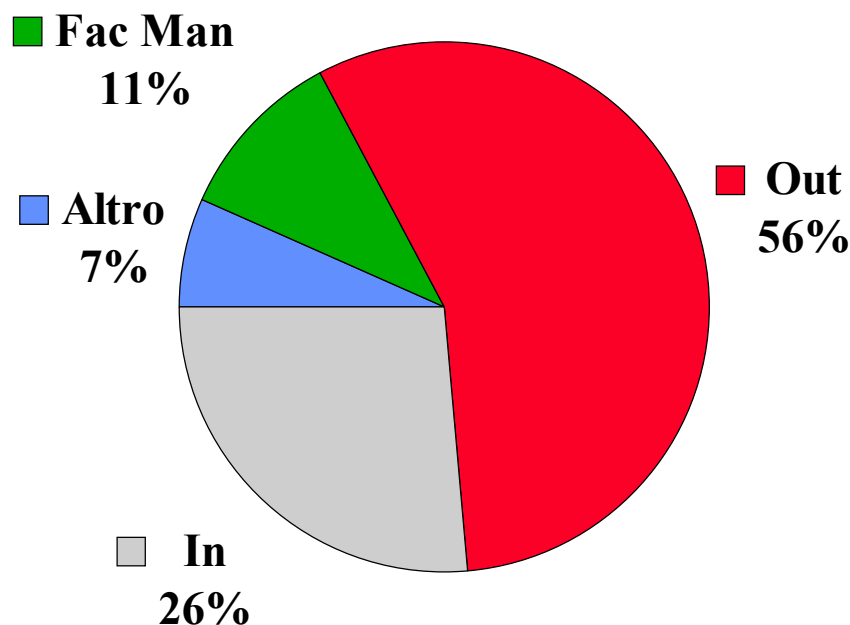
- monitorare costantemente l'evoluzione della domanda,
- sfruttare le opportunità comuni,
- produrre studi (GDL telecomunicazioni),
- promuovere e definire standard (Misura qualità SW applicativo ISO 9126, GDL *S.L.A.*).
- E' escluso ogni scopo di lucro (art. 4 dello statuto)

# Consortziati

- **CEDACRI NORD**
- **CEDACRI OVEST**
- **DEBIS**
- **EUROS**
- **EDS**
- **ISTISERVICE**
- **ETRURIA**  
**INFORMATICA**
- **ISIDE**
- **SEC**
- ***SECETI***

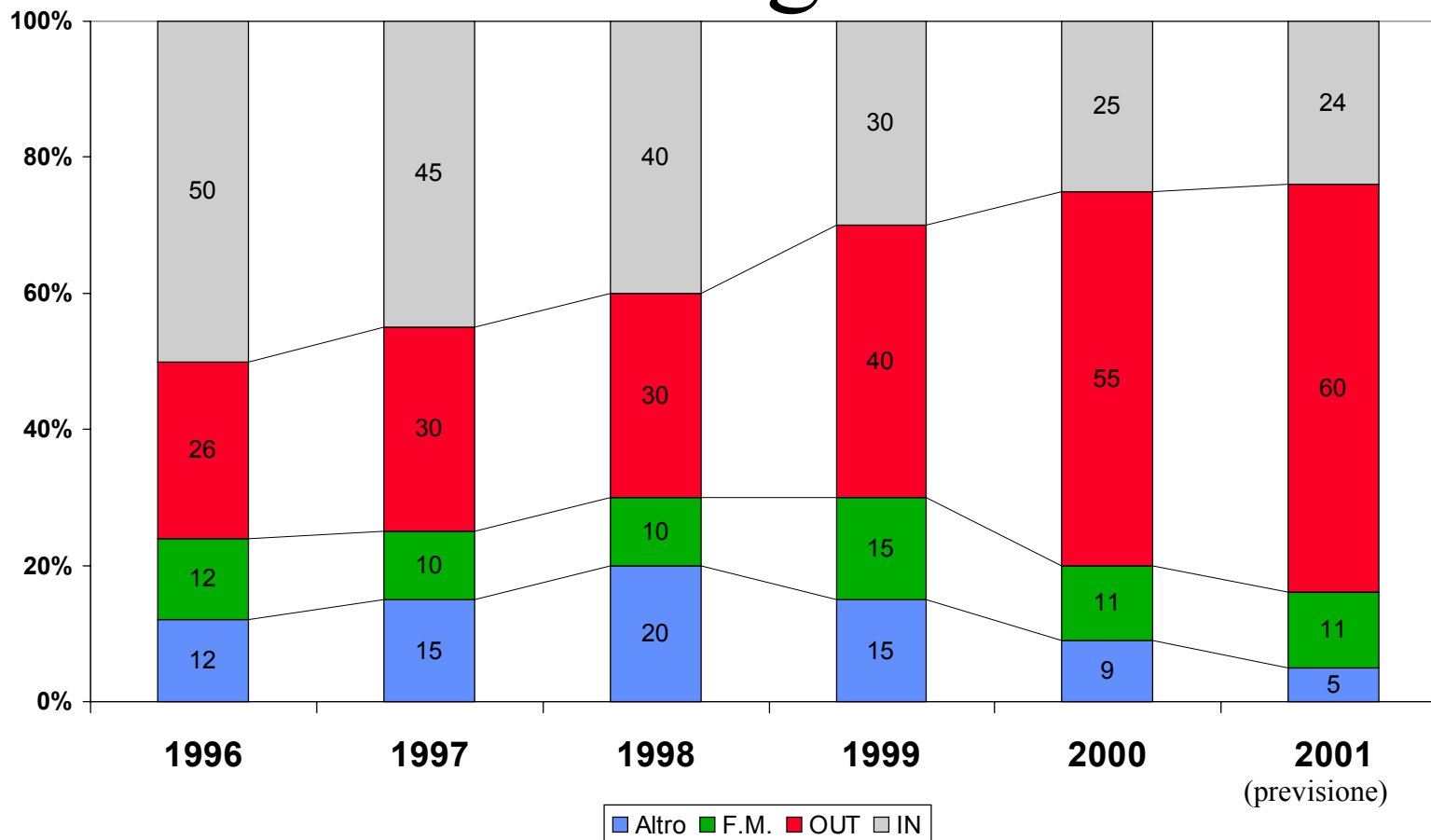
# L'outsourcing bancario

Situazione al 31/12/2000 secondo il Rapporto ABI CIPA  
“Rilevazione dello stato dell'automazione del sistema creditizio”



Campione: 121 banche pari al 74% dei fondi intermediati

# L'outsourcing bancario



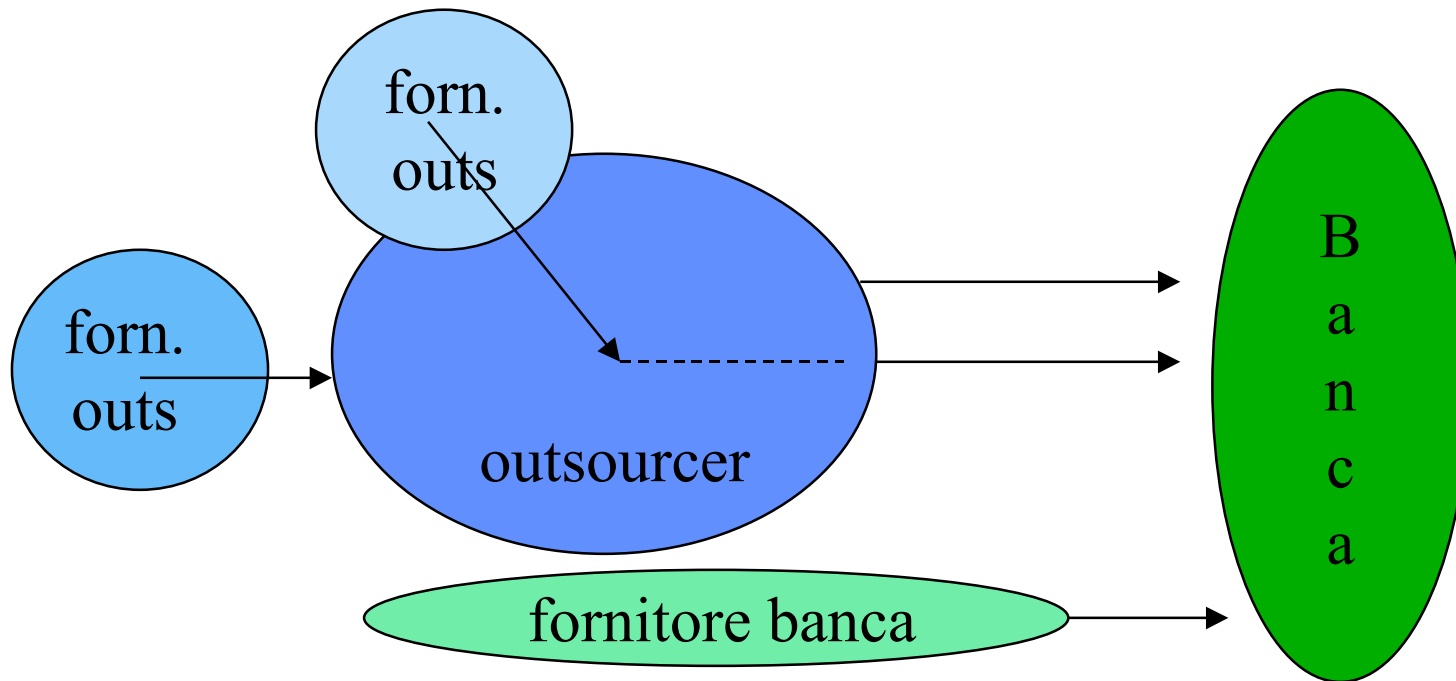
Campione: 78 banche che hanno sempre partecipato alla rilevazione

# Le problematiche di sicurezza

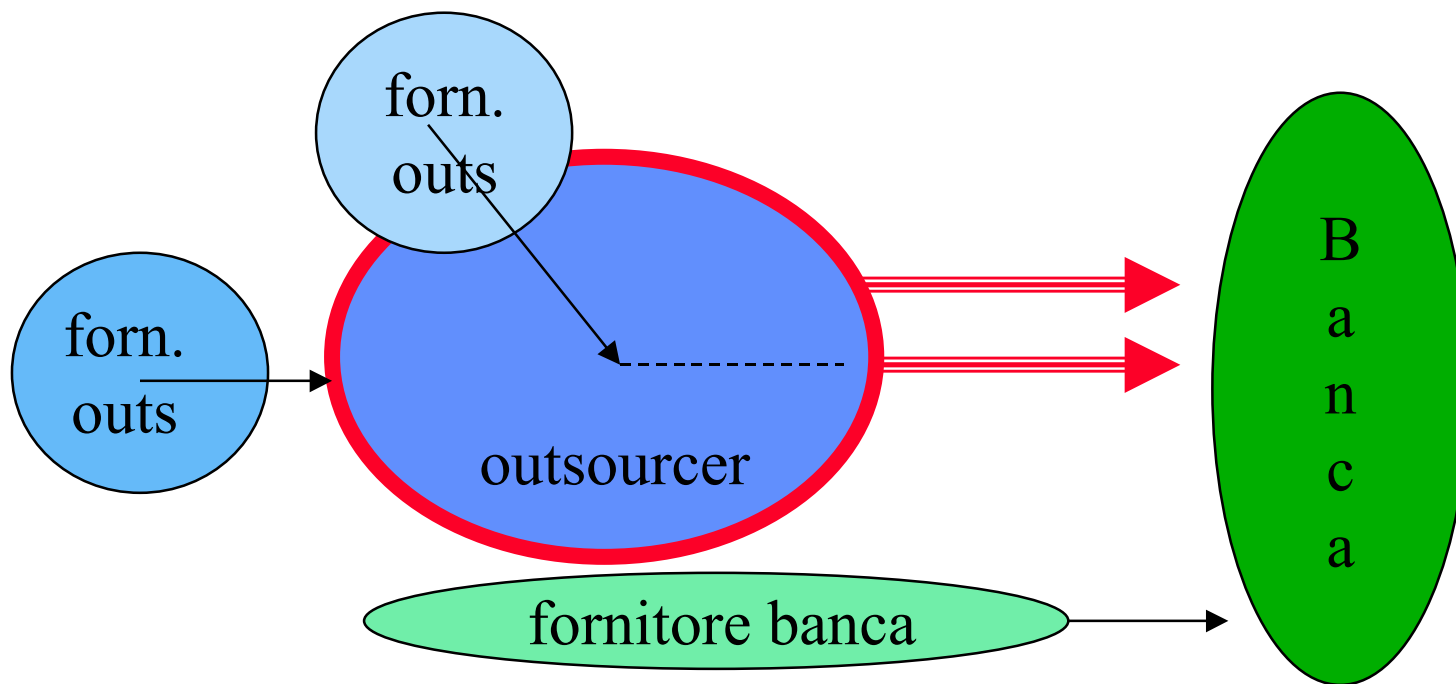
- L'outsourcing presenta problematiche di sicurezza più complesse rispetto alla gestione di un Centro di elaborazione dati interno ad un'azienda.
- La banca non può spossessarsi completamente delle responsabilità relative alla gestione dei suoi sistemi(\*).
- **La garanzia di sicurezza è parte integrante della relazione di trust che si deve stabilire tra banca cliente e fornitore di outsourcing.**

(\*) **Nuove Istruzioni di Vigilanza 9/10/98 – “L’attribuzione a soggetti terzi di attività connesse con il funzionamento dei sistemi informativi non esonera le banche dalle responsabilità di controllo.”**

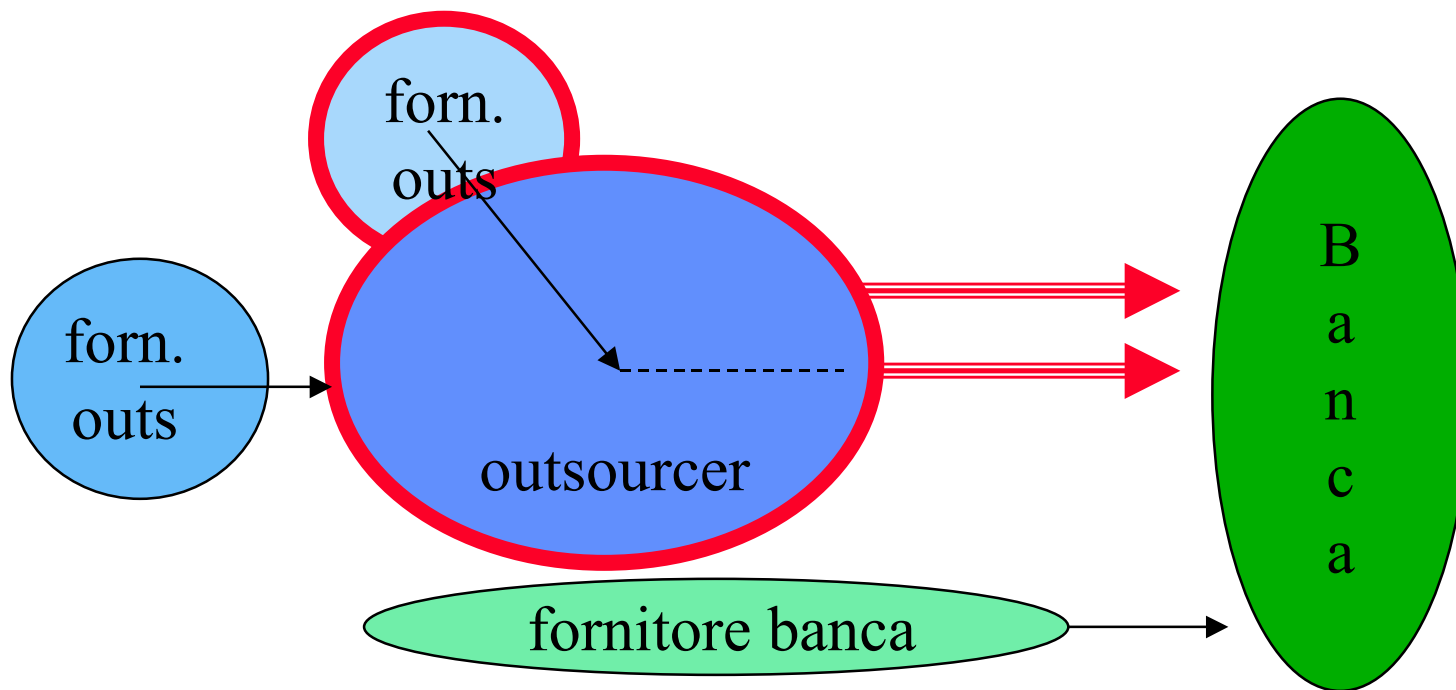
# I servizi



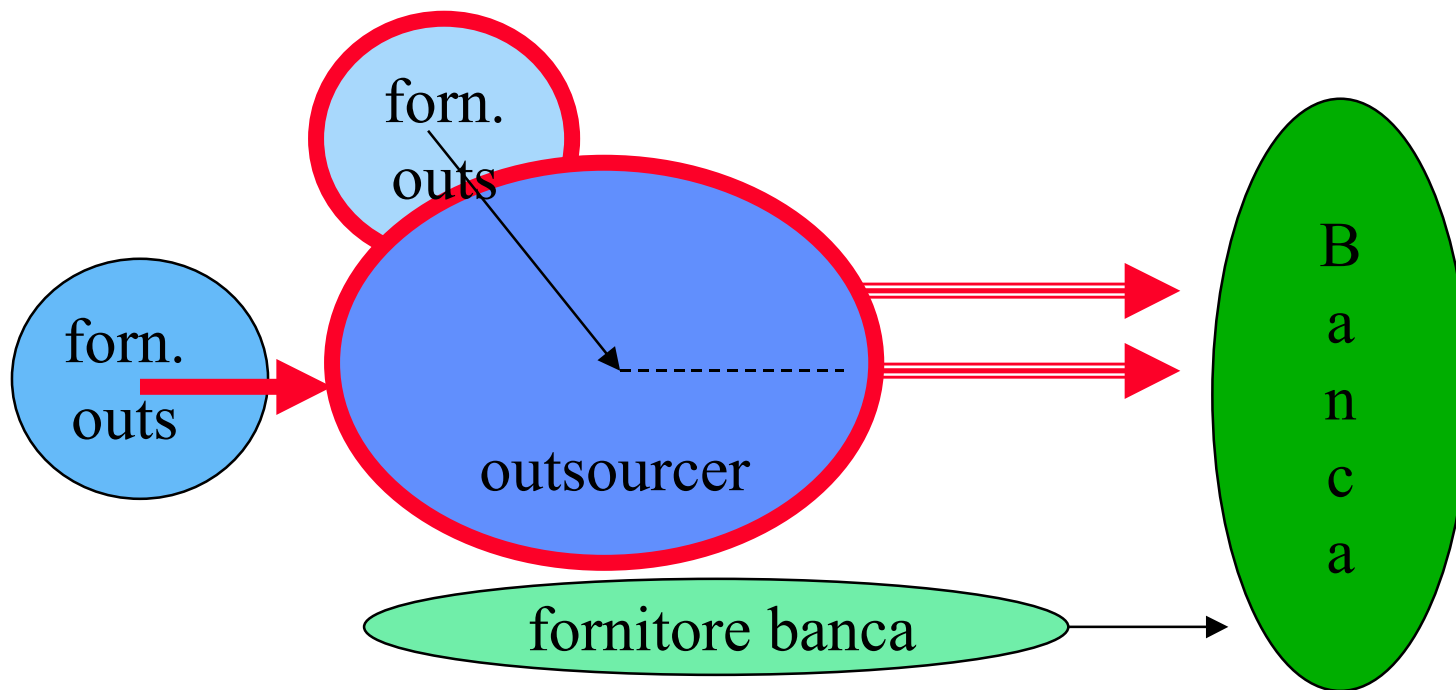
# La sicurezza dei servizi



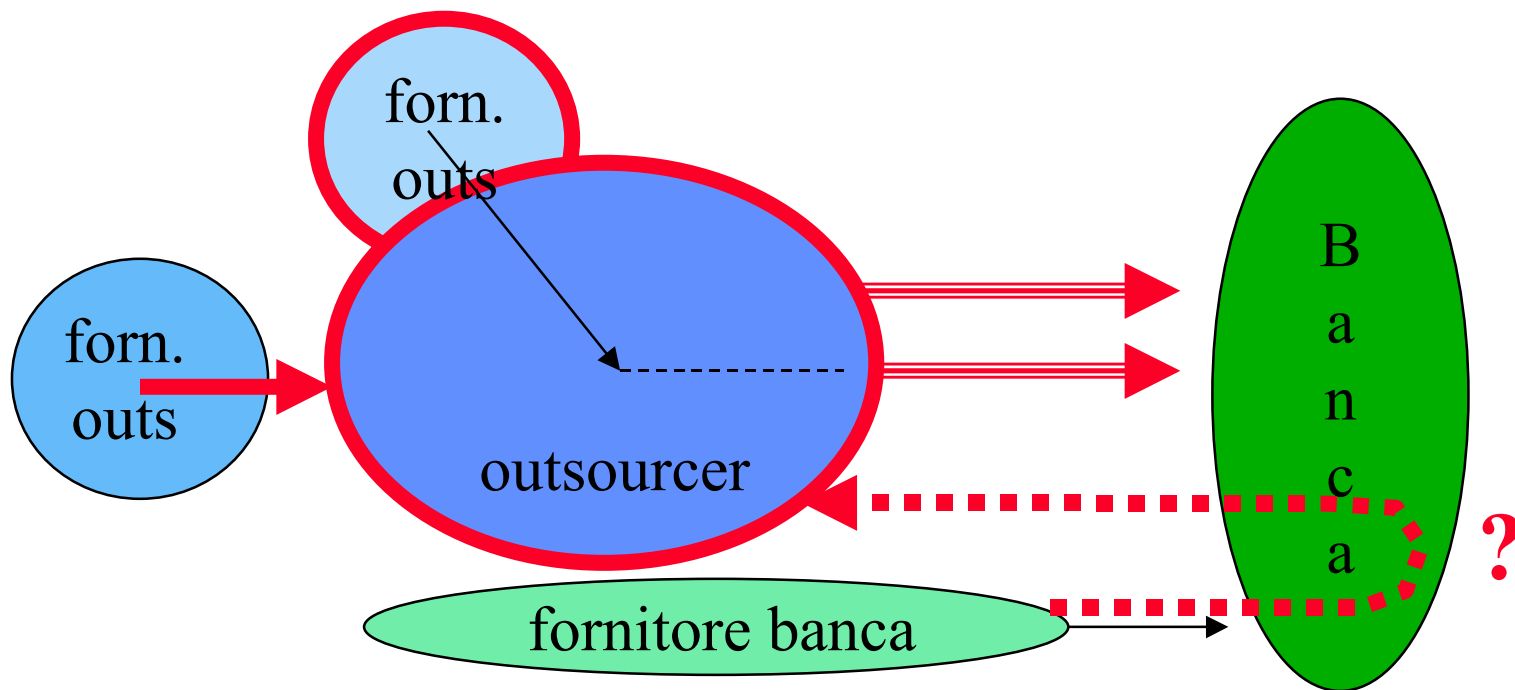
# La sicurezza dei servizi



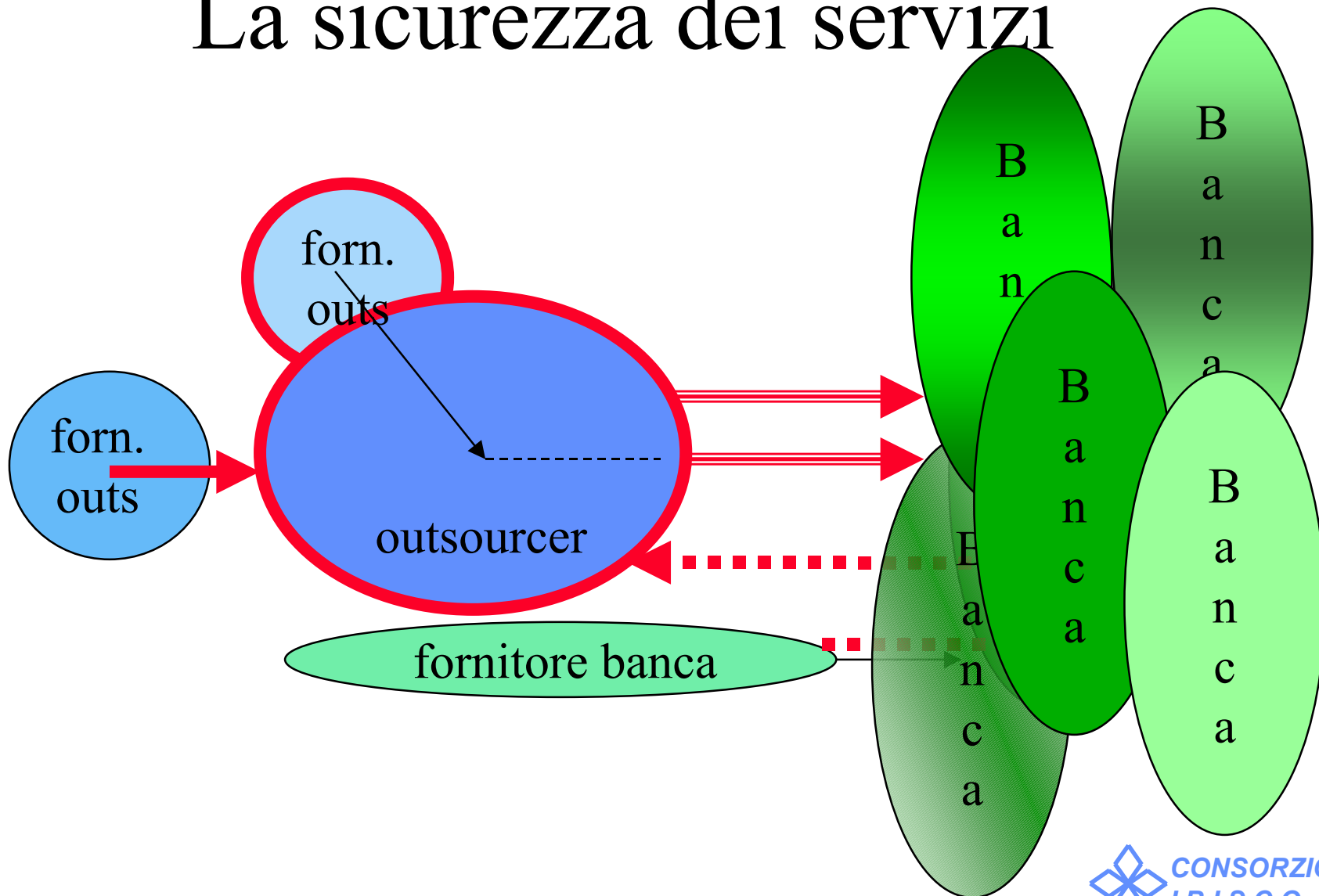
# La sicurezza dei servizi



# La sicurezza dei servizi



# La sicurezza dei servizi



# Come garantire la sicurezza

Occorre quindi distinguere tra:

1. **Ciò che è di totale responsabilità del fornitore del servizio**, che dovrà provvedere alla gestione delle apposite policy, da condividere con le banche clienti (p.e. la gestione della configurazione).
2. **Ciò che deve essere gestito direttamente dalla banca**, tramite gli strumenti messi a disposizione dal fornitore (p.e. l'abilitazione degli utenti).
3. **Le aree di totale responsabilità della banca** (p.e. la gestione delle stazioni di lavoro, del contante).

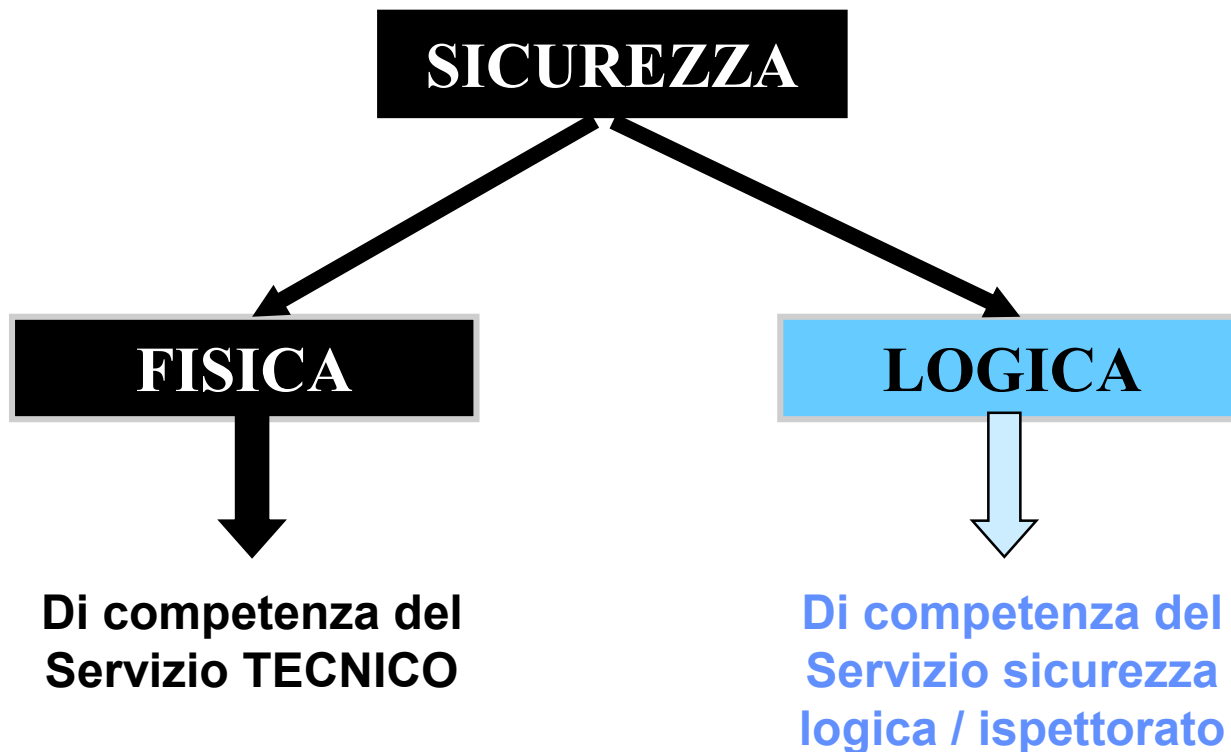
# Come garantire la sicurezza

- Anche se può sembrare banale, è indispensabile identificare chiaramente tutte le aree che possono avere impatti sulla sicurezza e definire a quale delle tre tipologie indicate appartengono.
- Occorre infine un lavoro di verifica sulla omogeneità dei livelli di sicurezza garantiti dall'applicazione delle regole così definite.

# *Security requirements in outsourcing contracts (da BS7799)*

- a) how the legal requirements are met;
- b) how is ensured that all parties involved, including subcontractors, are aware of their security responsibilities;
- c) how the integrity and confidentiality of the organization's business assets are to be maintained and tested;
- d) what physical and logical controls will be used to restrict and limit the access to information to authorized users;
- e) how the availability of services is to be maintained;
- f) what levels of physical security are to be provided;
- g) the right of audit.

# La gestione della sicurezza presso un fornitore (\*)



(\*) Le situazioni qui descritte non fanno riferimento specificatamente a nessun membro del Consorzio I.B.I.S.C.O. ma sono definite in base a quella che è la pratica corrente. Singoli membri possono offrire soluzioni anche considerevolmente diverse.

# Sicurezza fisica

Principali accorgimenti:

- SUDDIVISIONE fisica dei diversi ambienti.
- ROBOT per i nastri con tutte le caratteristiche di sicurezza.
- CAVEAU esterni per nastri di back-up.
- GUARDIE di custodia presenti 24 ore su 24 per 7 giorni (gestione delle emergenze, controllo degli accessi).
- Impianto antincendio / anti allagamento.

# Sicurezza fisica

Principali accorgimenti:

- **DISPONIBILITA'** di gruppi elettrogeni in caso di mancanza di energia elettrica.
- **IMPIANTO** di video registrazione per i punti vitali interni ed esterni.
- **CONTROLLO** accessi regolamentato da badge, con suddivisione di zone e fasce orarie in base alle mansioni.
- **DIFESA FISICA** delle risorse di maggiore rilevanza (anche contro eventi accidentali come l'urto di un muletto).

# Sicurezza logica

Principali accorgimenti:

- Definizione di **una policy di sicurezza globale**, approvata dal CdA, che prevede la definizione delle diverse figure professionali e gli specifici doveri (p.e. l'utente deve sempre autenticarsi con il proprio l'identificativo e password, non deve accedere a programmi / dati senza uno specifico incarico, è vietato modificare la configurazione hardware e software del proprio posto di lavoro).
- Al crescere del livello professionale e di responsabilità dell'utente i compiti vengono dettagliati in misura minore e viene richiesta una attività di controllo e prevenzione di eventuali abusi.

# Sicurezza logica

Principali accorgimenti:

- Gestione tramite **specifici regolamenti** di tutte le azioni di tipo specialistico (p.e. accesso alle informazioni registrate dall'impianto di video sorveglianza, modalità di distruzione dei supporti magnetici, accesso ai locali).
- È sempre indicata la funzione responsabile di ogni attività, *evitando di specificare in quale maniera e quando è possibile richiedere eventuali eccezioni.*
- Ogni regolamento indica una data entro la quale deve essere rivisto.

# Sicurezza logica

## Principali accorgimenti:

- La scrittura dei regolamenti è a carico del fornitore dei servizi di outsourcing.
- Per tutte le aree che vedono coinvolte le banche clienti, viene incaricato della verifica / approvazione un comitato degli utenti.

# Sicurezza logica

L'accesso ad host e' regolamentato da prodotti specifici che controllano chi accede a:

- transazioni
- programmi
- archivi, ecc.

Fa parte dei documenti condivisi con le banche la definizione dei profili di accesso.

# Sicurezza logica

La gestione e la distribuzione delle abitazioni è un compito specifico delle banche che gestiscono in autonomia:

- L'abilitazione e il blocco degli utenti;
- Lo sblocco delle password
- Le variazioni di funzioni

Nel caso sia necessario definire i nuovi profili di abilitazione, la decisione è presa in accordo con il fornitore di servizi.

# Sicurezza logica

Viene mantenuto un log per il controllo di tutti gli eventi significativi come:

- Variazioni alle abilitazioni degli utenti.
- Violazioni degli utenti.

Sono mantenuti archivi storici con la possibilità di ottenere statistiche periodiche.

# Sicurezza logica

La separazione degli archivi tra le diverse banche che utilizzano il sistema è uno dei punti chiave della sicurezza offerta:

- Viene sempre verificata la congruenza fra il codice dell'utente che richiede la transazione e i codici degli archivi contenenti i dati.
- Le transazioni dispositive vengono loggate.
- In alcuni casi vengono loggate anche le transazioni di interrogazione.

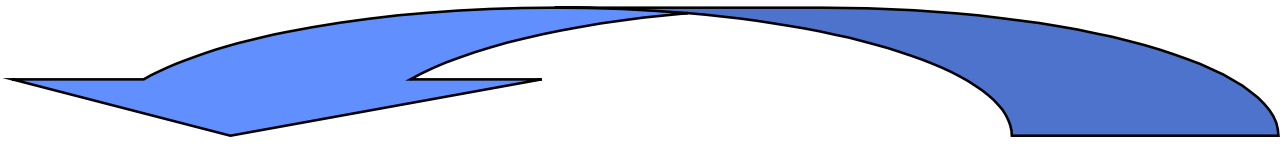
# Sicurezza – i punti di forza

Come per il sistema informativo messo a disposizione delle banche, la gestione della sicurezza all'interno di un fornitore come quelli appartenenti al Consorzio I.B.I.S.C.O. garantisce innanzitutto la gestione “ industriale “ del problema.

Le dimensioni delle aziende consentono sempre approcci al massimo livello della conoscenza.

È importante lo scambio di informazioni e di idee che avviene all'interno dei comitati utenti.

# Sicurezza – il futuro



**I clienti sono sempre più attenti alle problematiche attinenti la sicurezza e cominciano a percepirne il valore economico.**

**Per le aziende di outsourcing la sicurezza è sempre più un elemento di business.**

# Sicurezza – nuovi rischi

Le sfide non mancano, per citare i punti di maggiore attenzione possiamo indicare :

- Il passaggio da reti di trasmissione dati costruite su linee dedicate e con protocolli specifici, all'uso di standard di mercato su reti private virtuali.
- La sempre maggiore “connessione” tra applicazioni, sistemi, utenti, aziende rende spesso difficile una compartimentazione del rischio.
- Il sempre maggior valore delle informazioni rispetto agli “oggetti” orienterà sempre di più la criminalità verso questi beni.

# Sicurezza – nuove opportunità

Per la parte positiva possiamo citare:

- La possibilità, grazie alla firma digitale, di gestire in maniera sicura documenti e credenziali elettroniche.
- La possibilità di ricorrere a tecniche crittografiche integrate (p.e. nei dispositivi di telecomunicazioni).
- La percezione del valore della sicurezza da parte dei fornitori, assieme allo spettro di una possibile “liability”, incrementerà l’offerta di sistemi più sicuri.

# Il futuro ...

La previsione del futuro è sempre stata una attività altamente rischiosa e incerta, ma sono sicuro di una cosa: sarà ricco di nuove sfide e, in una parola, sicuramente **stimolante.**

## **Estote parati!**

Grazie per l'attenzione

**Arturo Salvatici**

arturo.salvatici@seceti.it