Direzione Centrale Organizzazione e Sistemi Informativi

Dirigente Area Sicurezza ICT e Privacy
dr Mario Cilla

Roma 23/05/2018

Obiettivo

1. Consentire l'analisi delle banche dati INPS per lo studio dei fenomeni del mondo del lavoro e della previdenza salvaguardando la riservatezza dei dati personali
2. Consentire la correlazione di banche dati appartenenti a diversi soggetti, pubblici o privati, salvaguardando la riservatezza reciproca delle rispettive banche dati.

1.1 Processo di data masking

Area Sicurezza ICT e Privacy

Ricercatore:

- Esprime i fabbisogni informativi

Analista dati INPS:

- Verifica la «necessità» degli attributi richiesti per le finalità della ricerca
- Identifica gli archivi sorgenti
- Analizza i dataset risultanti con i criteri selettivi indicati
- Identifica gli attributi che possono consentire l'identificazione dell'interessato
- Analizza la cardinalità degli attributi del dataset risultante per prevenire l'identificazione, anche indiretta, dell'interessato
- Effettua la pseudoanonimizzazione degli attribuiti identificati che, in maniera diretta o indiretta, potrebbero ricondurre all'identificazione degli interessati (si adottano tecniche di hashing con SALT che resta noto solo all'analista INPS)

1.2 Processo di data masking
(correlazione con dataset esterni)

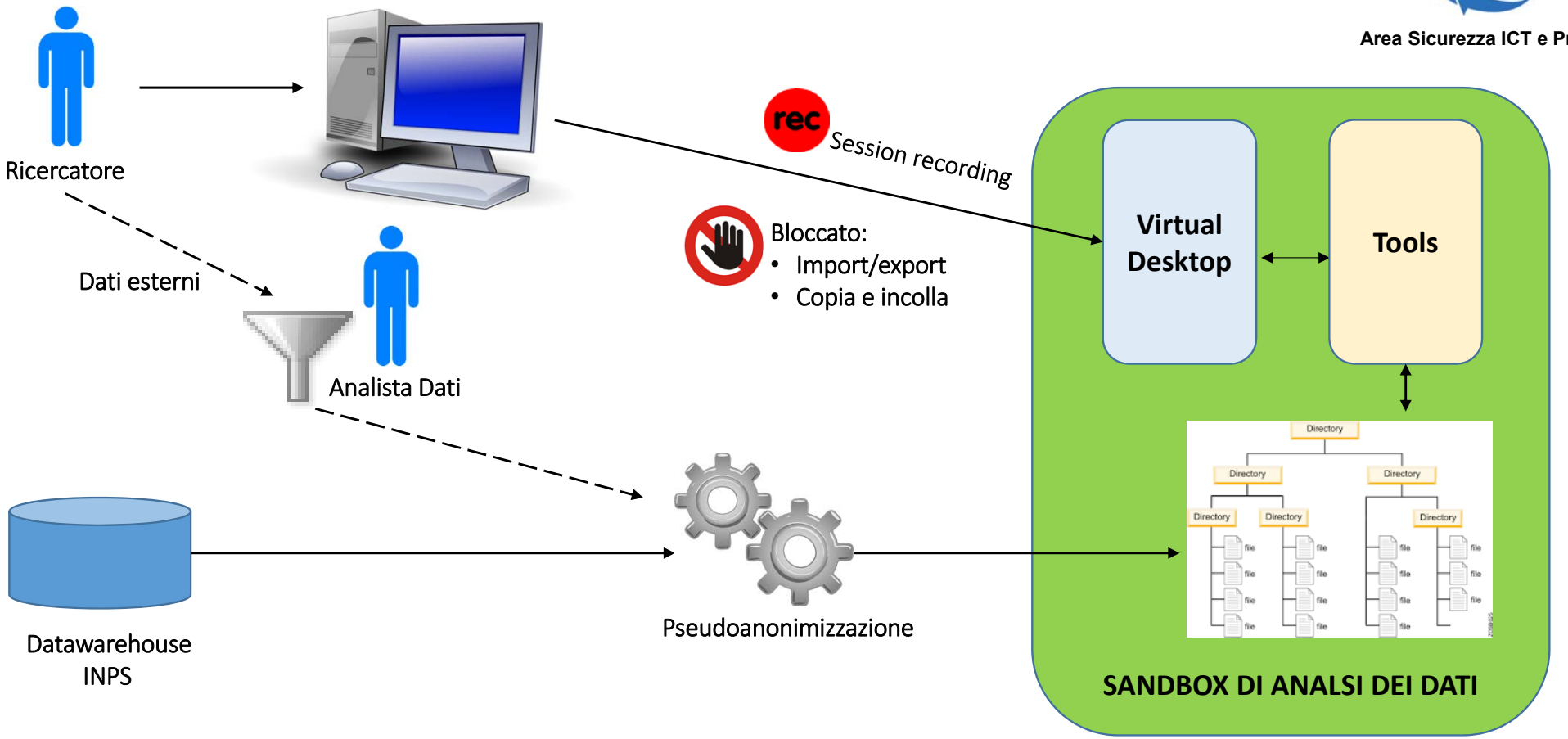
Area Sicurezza ICT e Privacy

Qualora il ricercatore abbia la necessità di correlare i dati aziendali con dataset esterni nelle sue disponibilità, si procederà:

- alla loro pseudoanonimizzazione con gli stessi algoritmi impiegati per i dati aziendali se gli attributi da importare hanno valori con scarsa variabilità rispetto alla cardinalità del dataset.
- alla loro pseudoanonimizzazione con diverso algoritmo se i dati importati possono rilevare l'identità degli interessati se associati a dati aziendali non di interesse per la ricerca (anonimizzazione di dominio).
- Non si procede all'importazione se le «tuple» da importare hanno un'alta variabilità di valori e tali da costituire una chiave secondaria per l'identificazione dei soggetti a cui si riferiscono.

1.3 Trattamento dei dati

Area Sicurezza ICT e Privacy

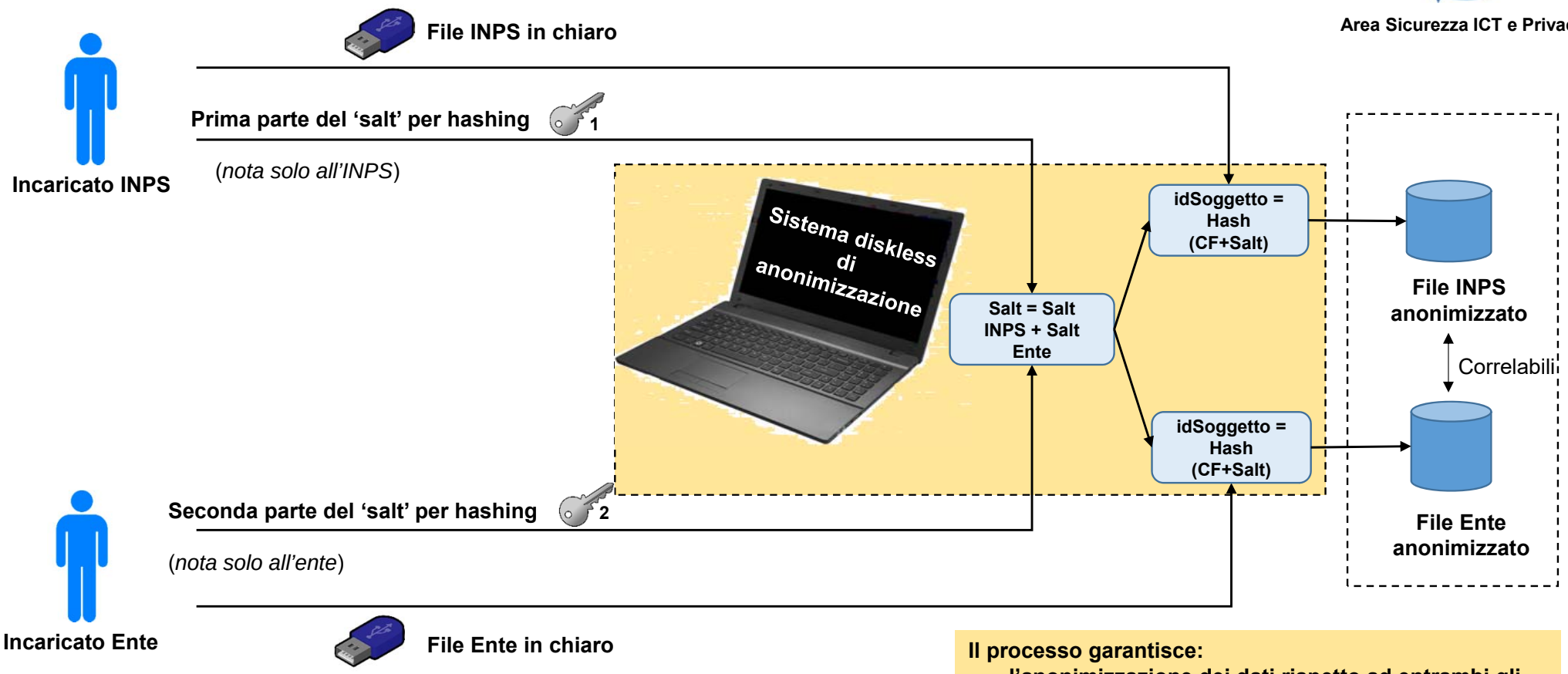


2 Correlazione con banche dati esterne

Consentire la correlazione di banche dati appartenenti a diversi soggetti, pubblici o privati, salvaguardando la riservatezza reciproca delle rispettive banche dati.

2.1 Processo di anonimizzazione a N fattori

Area Sicurezza ICT e Privacy

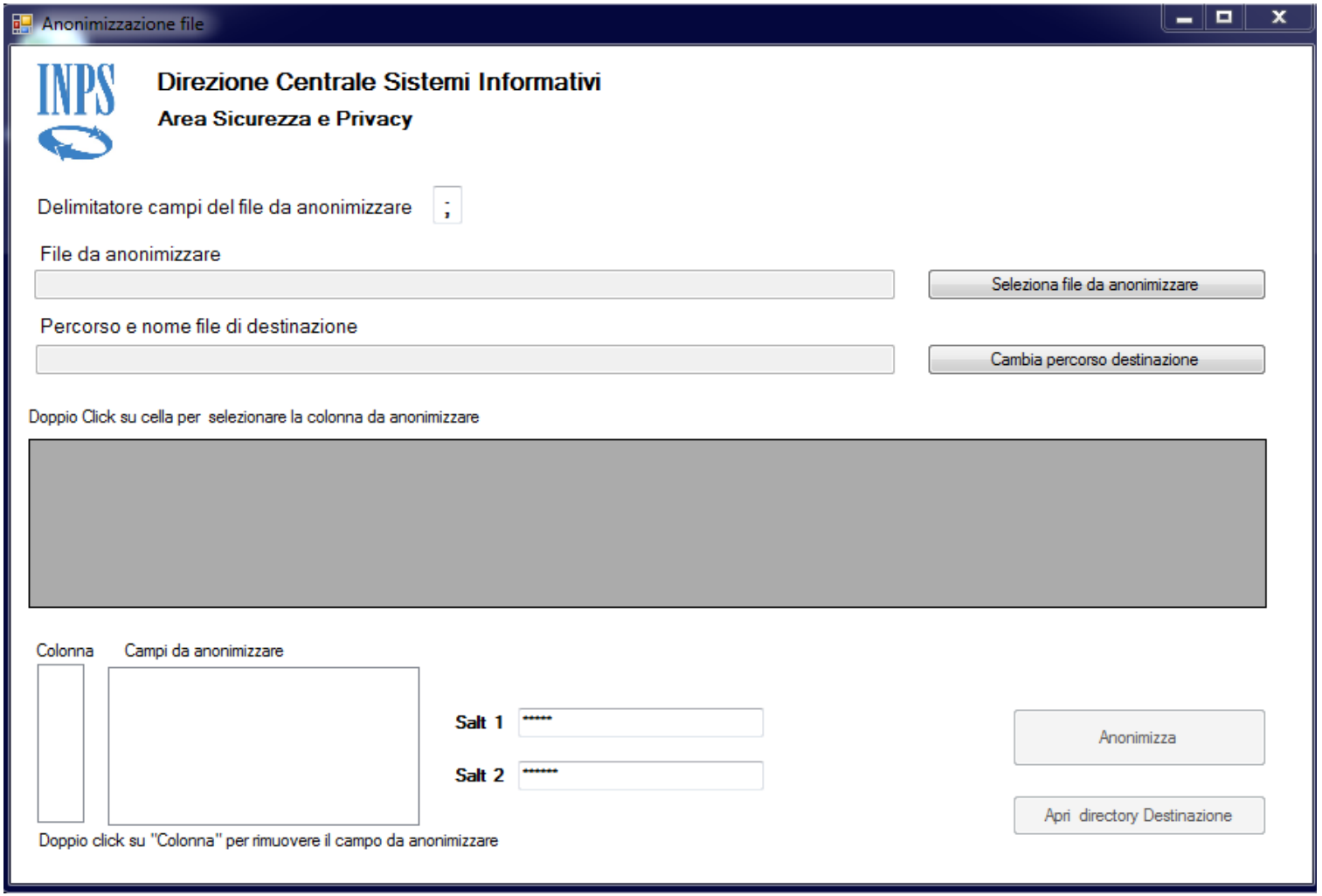


Il processo garantisce:

- **l'anonimizzazione dei dati rispetto ad entrambi gli attori poiché ognuno conosce solo metà del salt segreto**
- **La correlabilità dei due archivi**

2.2 Software di anonimizzazione a N fattori

Area Sicurezza ICT e Privacy



CD Live

2.3 Software di anonimizzazione a N fattori

Area Sicurezza ICT e Privacy

E’ strettamente necessaria una attenta analisi preliminare degli attributi messi a fattor comune dalle due parti per prevenire il rischio che:

- Il subset di attributi di ogni ente possa ricondurre all’identificazione degli interessati
- il set completo di attributi possa ricondurre all’identità dell’interessato

Conclusioni

Area Sicurezza ICT e Privacy

Le soluzioni devono necessariamente interessare i seguenti ambiti:

- Misure tecniche
- Misure organizzative
- Attenta analisi dei dati