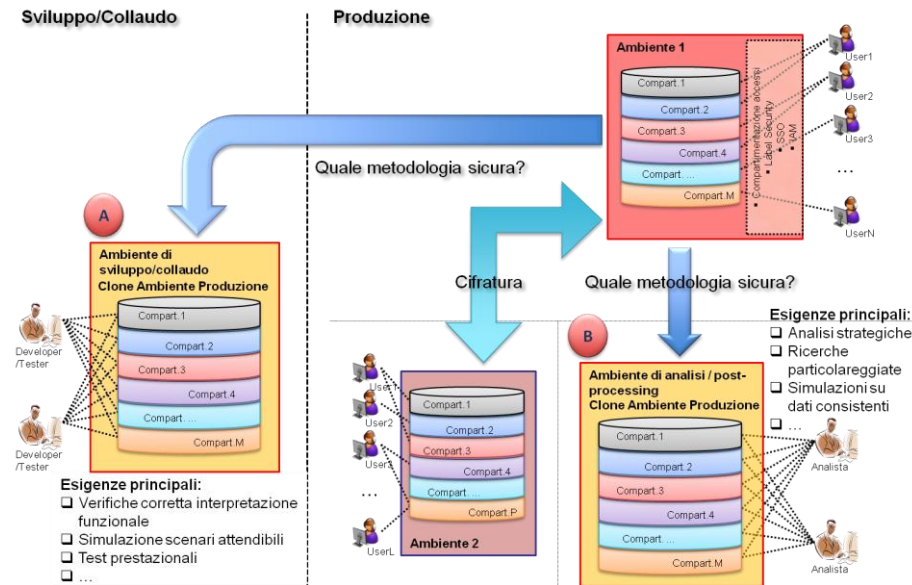


## Overview

Circa il 60% delle aziende copia i dati dagli ambienti di produzione in ambienti extra (A) e post produzione (B) per supportare attività di sviluppo, test e analisi statistiche di vario tipo, mettendo a repentaglio la riservatezza dei dati d'origine. Ciò comporta la divulgazione, seppur non intenzionale, di dati sensibili o riservati a categorie di operatori non autorizzati al trattamento.



Sviluppatori, personale addetto alla quality assurance, alla formazione e alle analisi statistiche, pur non evidenziando la necessità di disporre di buona parte dei dati sensibili o riservati originari, devono poter contare sulla disponibilità di dati realistici che rispettino le regole semantico / sintattiche, l'integrità referenziale, la coerenza e le regole di business applicabili sui dati reali.

Per assicurare il mantenimento della confidenzialità delle informazioni e la compliance a standard e normative, è necessario limitare l'accesso ai dati (in particolar modo a quelli sensibili) ai soli utenti che ne hanno un'inderogabile necessità (**need to know**) e nei limiti strettamente necessari per l'adempimento delle mansioni previste (**least privilege**).

## Perché adottare una soluzione di Data Masking ?

Il dato in un ambiente extra e post produzione è esposto a rischi aggiuntivi, essendo accessibile da altre categorie di operatori quali sviluppatori, analisti e collaudatori ed a cicli di gestione meno rigidi di quelli di produzione.

**Minore esposizione al rischio**

**Minori costi di compliance**

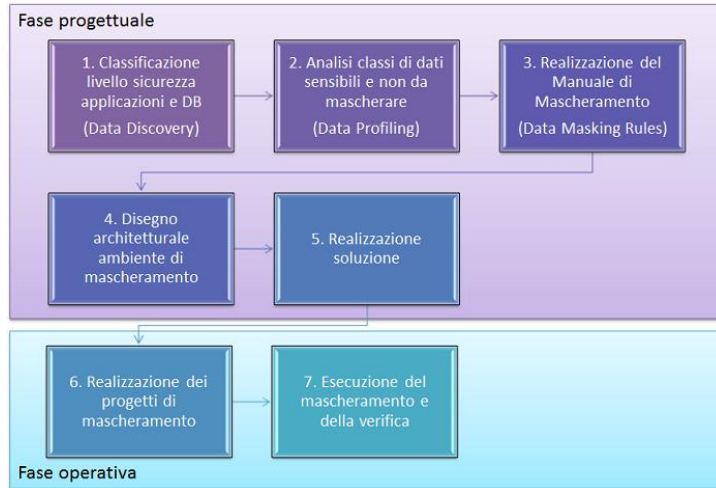
Il depotenziamento del dato in ambiente extra e post produzione rende superflua l'adozione di procedure particolarmente costose

La desensibilizzazione dei dati ne agevola l'utilizzo in ambienti differenti da quelli di produzione, rendendo possibile il ricorso ad esternalizzazioni ed a staff aggiuntivo

**Maggiore reattività**

Present affronta il problema della gestione degli ambienti di sviluppo e collaudo con una soluzione di *Data Masking* sviluppata per indirizzare le esigenze di sicurezza dei dati sensibili e di rappresentatività degli ambienti

**La soluzione**



**L'approccio Present** è basato su step metodologici, collaudati e consolidati, frutto dell'esperienza maturata in ambito Security Management e Quality Assurance.

L'obiettivo è assicurare la *gestione dell'intero ciclo di vita del mascheramento dati (Data Masking Lifecycle Management)*.

**PRIVATE** è la **soluzione Present** per il **Data Masking**, basata su prodotti leader di mercato, adattabile alle diverse esigenze dei clienti, i cui moduli principali sono:

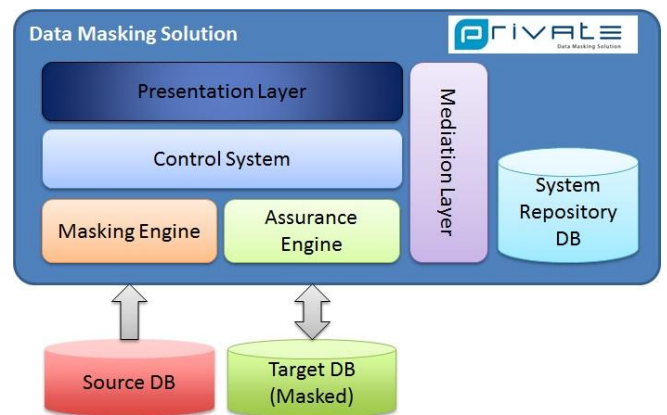
**Presentation Layer:** interfaccia web del sistema.

**Control System:** orchestra il processo di mascheramento definendo le regole generali, i responsabili designati e mantenendo un log delle attività.

**Data Masking Engine:** effettua il mascheramento dei dati nei termini prescritti dal Control System.

**Assurance Engine:** verifica che la somiglianza tra le due basi dati sia inferiore alle soglie considerate accettabili.

**Mediation Layer:** middleware per la gestione dell'integrazione tra i moduli del sistema e con i sistemi esterni.



**L'Offerta Present in ambito Data Masking** consiste nella soluzione tecnologica **PRIVATE** corredata dai diversi servizi professionali di *Consulenza, System Integration e Service Management*, finalizzati a supportare il cliente durante tutte le fasi preliminari di analisi del problema e definizione dei requisiti di mascheramento dati, di configurazione, personalizzazione ed integrazione della soluzione Private nel proprio contesto, di gestione operativa ed evolutiva della soluzione tecnologica rilasciata.

Present affianca altresì il cliente nella *gestione di tutte le problematiche di compliance* offrendo supporto per la revisione degli adempimenti previsti dalla normativa in essere e per il miglioramento del sistema di governo della sicurezza, offrendo un programma coordinato di servizi di tutoring e formativi.