ZUCCHETTI

GDPR

Tutelate: Le persone fisiche

Oggetto di tutela: I dati Personali

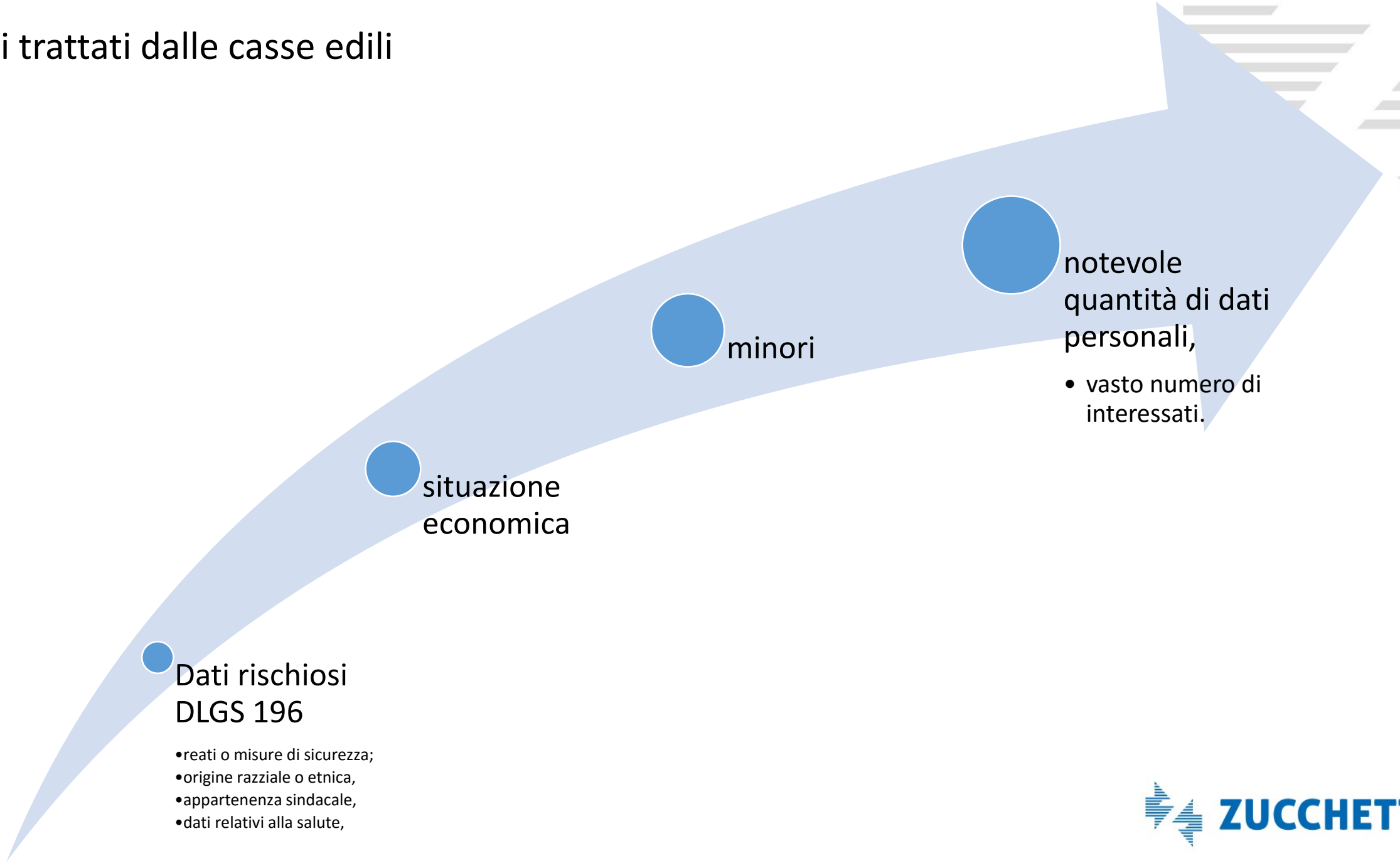
Categoria di dati particolari
Dati Identificativi

- Dati sensibili / rilevanti
- Dati giuridici
- Dati che presentano rischi specifici per i diritti e le libertà degli interessati

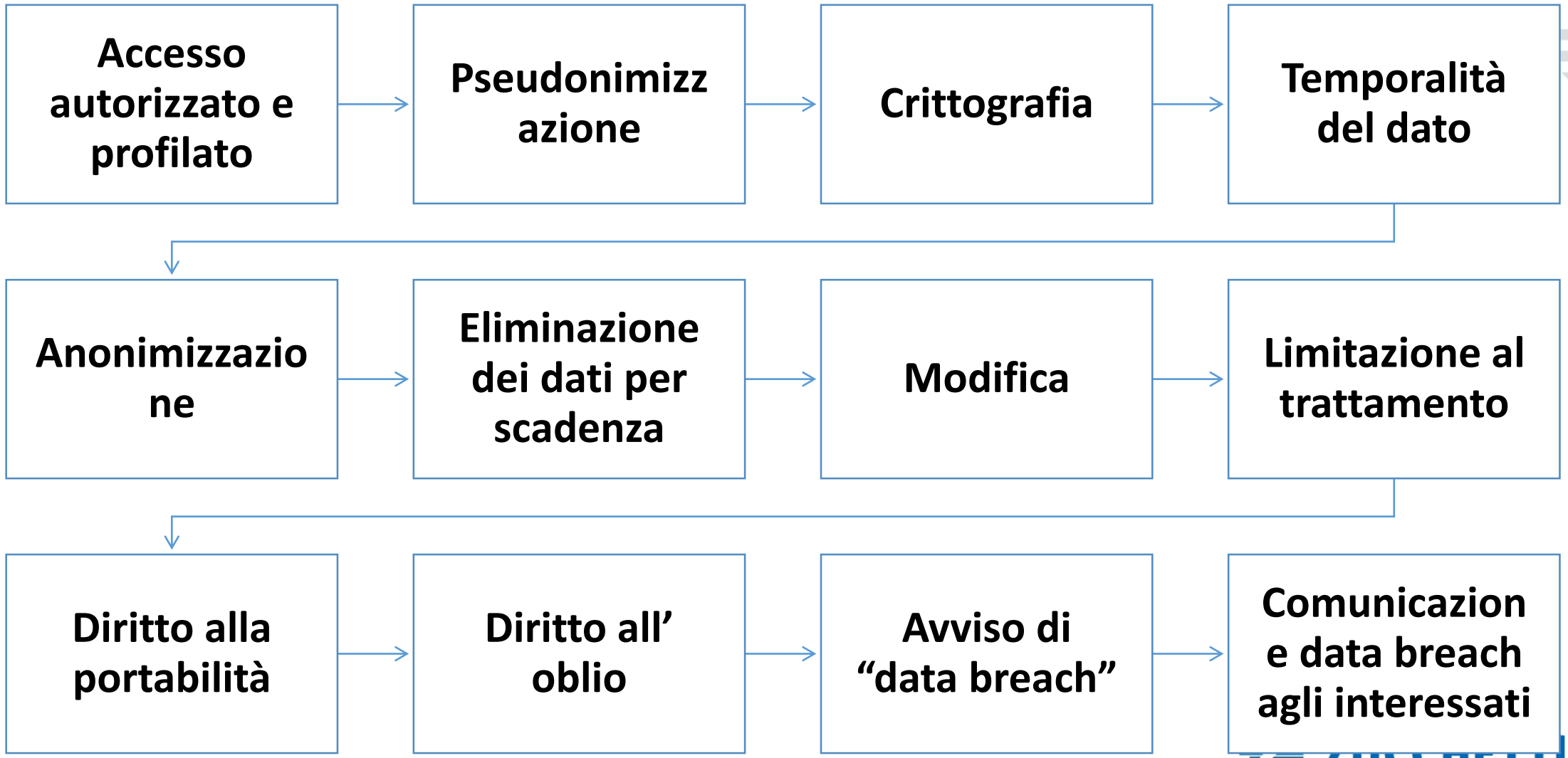
Tra questi vi sono categorie di dati personali che presentano rischi specifici:

- origine razziale o etnica,
- opinioni politiche,
- convinzioni religiose o filosofiche,
- appartenenza sindacale,
- dati genetici,
- dati relativi alla salute,
- dati relativi alla vita sessuale,
- condanne penali,
- reati o misure di sicurezza;
- valutazione di aspetti personali,
- valutazione rendimento professionale,
- situazione economica,
- preferenze o gli interessi personali,
- affidabilità o il comportamento,
- ubicazione o gli spostamenti,
- minori;
- notevole quantità di dati personali,
- vasto numero di interessati.

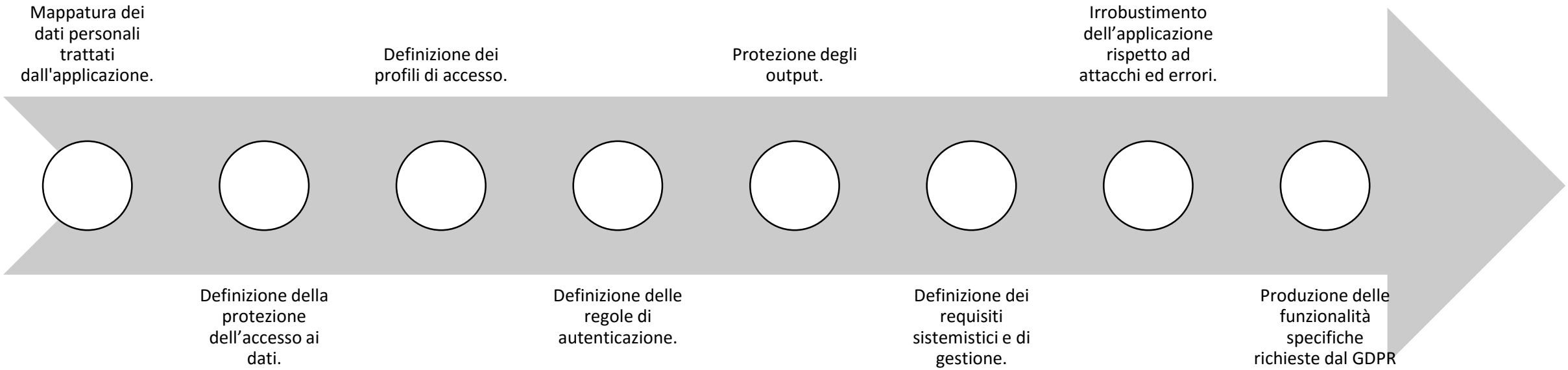
Dati trattati dalle casse edili



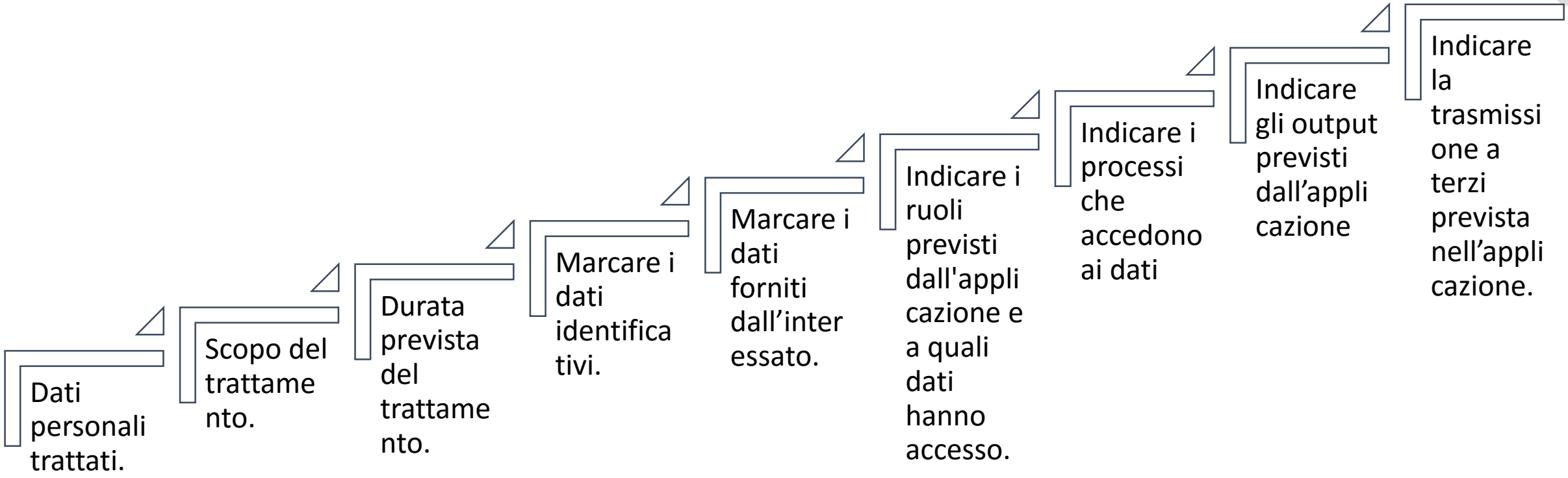
Misure a tutela dei dati



I sistemi informativi a servizio del Titolare



Mappatura dei dati personali trattati dall'applicazione

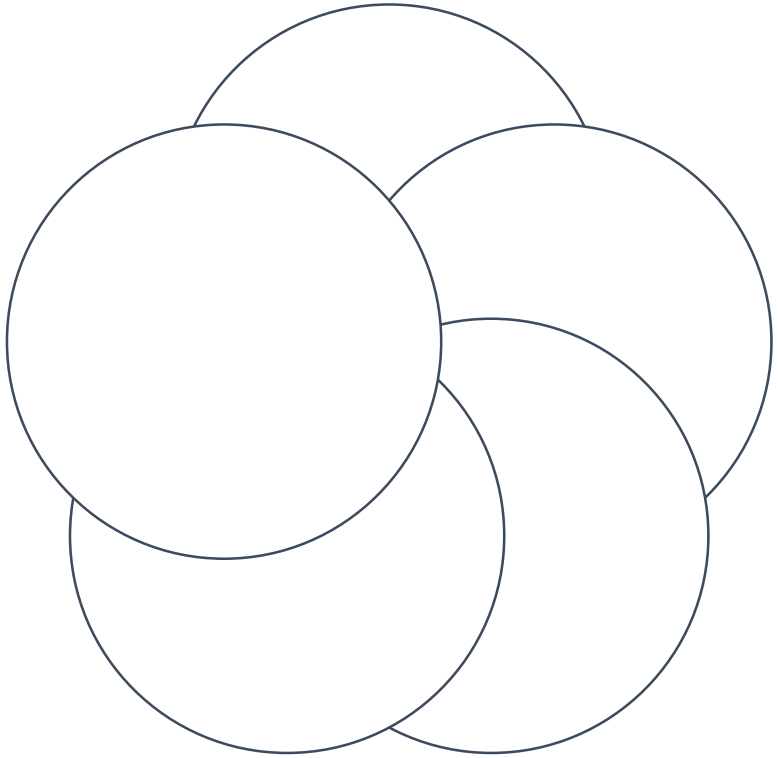


Operatività del sistema

Scopo e liceità

Minimizzazione

- nel dato
- nell'uso
- nel tempo



Rischio

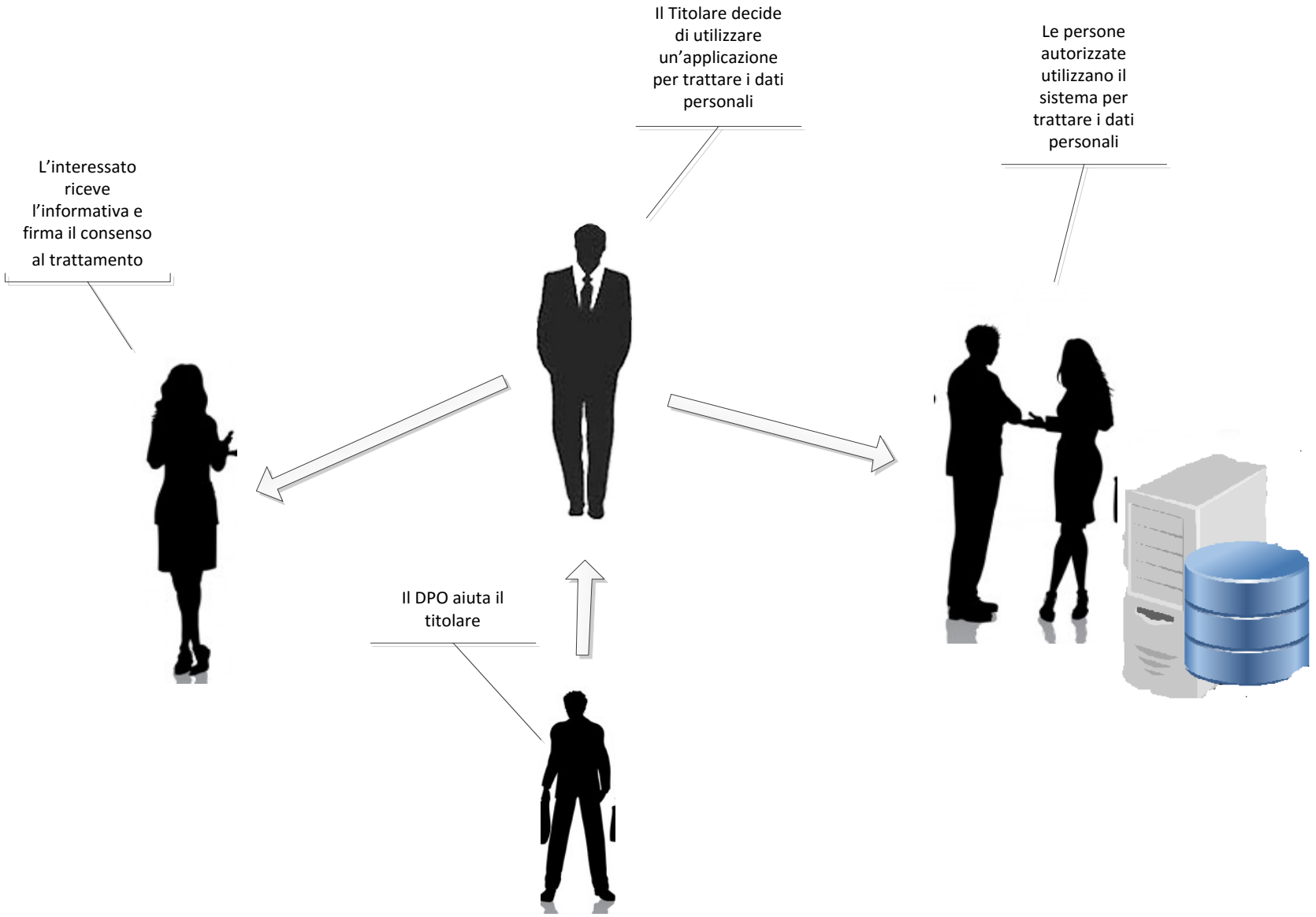
Mappatura delle trasmissioni a terzi

Mappatura degli output

ZUCCHETTI

Le relazioni ed i ruoli nei trattamenti dei dati

TITOLARE CHE ESEGUE I TRATTAMENTI CON UN FOGLIO DI EXCEL

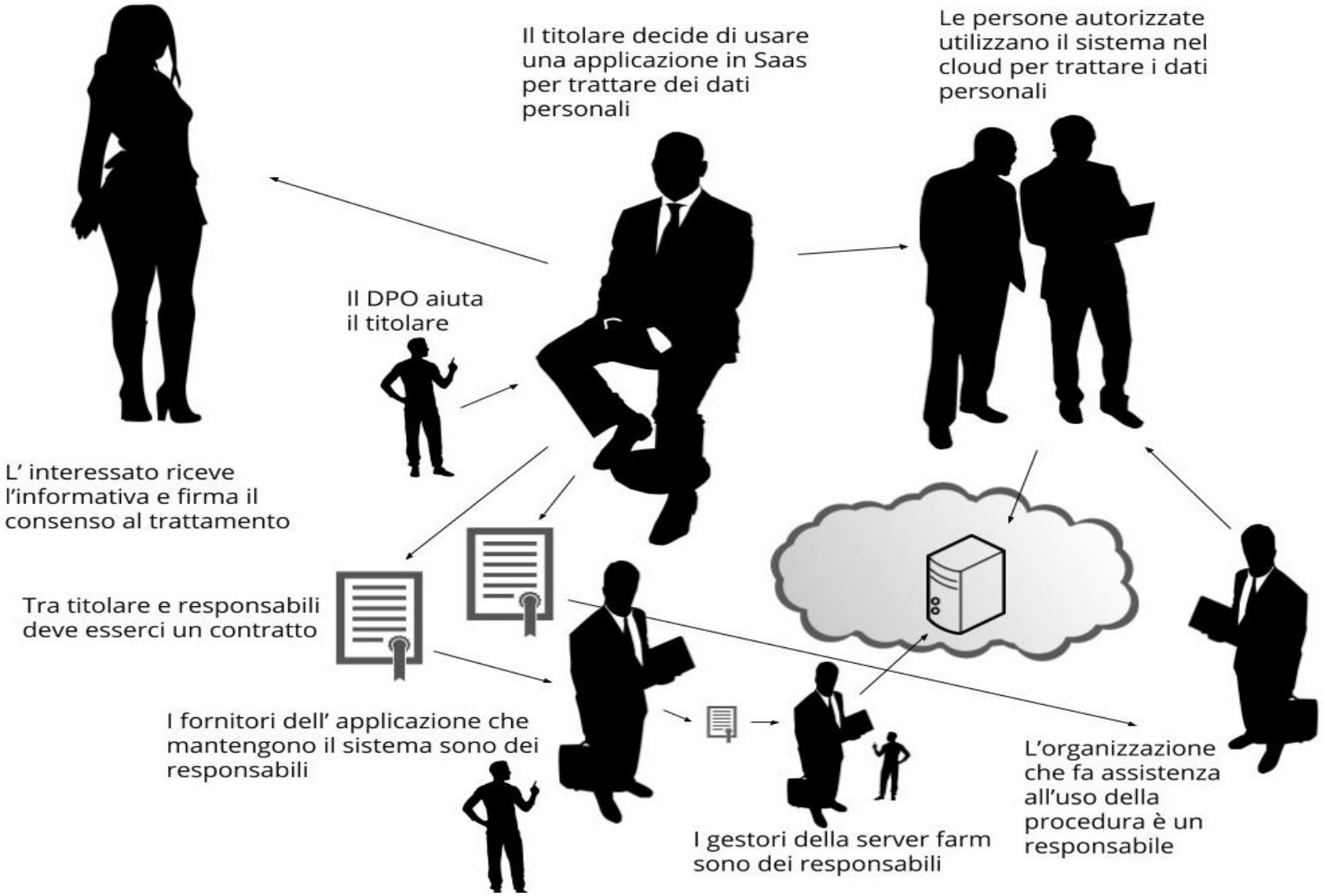


COMPITI DEL TITOLARE

- DEFINIRE LE MODALITA' DEL TRATTAMENTO
- ANALIZZARE I RISCHI DERIVANTI DAL TRATTAMENTO
- PROGETTARE LE MISURE DI SICUREZZA ADEGUATO NELLO SPIRITO DELLA «PRIVACY BY DESIGN»
  (PROTEGGERE IL FOGLIO EXCEL – CIFRATURA; PROTEGGERE IL COMPUTER IN CUI E' ARCHIVIATO CON LIMITAZIONE DI ACCESSO SOLO ALLE PERSONE AUTORIZZATE)
- DECIDERE IL CICLO DI VITA DEI DATI: PER QUANTO TEMPO SARANNO CONSERVATI E COME VERRANNO CANCELLATI
- ORGANIZZARE LA RACCOLTA DEL CONSENSO E DELLA DISTRIBUZIONE DELL'INFORMATIVA
- AUTORIZZARE LE PERSONE ALL'ESECUZIONE DELLA RACCOLTA E DELLA GESTIONE
- FORMARE LE PERSONE SULLE MISURE DI SICUREZZA DA ATTUARE E RISPETTARE
- TENUTA DEL «REGISTRO DEL TITOLARE»
- NOMINARE IL DPO (DATA PROTECTION OFFICER) PER I TRATTAMENTI CHE LO RICHIEDONO

ZUCCHETTI

TITOLARE CHE ESEGUE TRATTAMENTI ATTRAVERSO UN SERVIZIO CLOUD



ZUCCHETTI

COMPITI DEL TITOLARE

- DEFINIRE LE MODALITA' DEL TRATTAMENTO
- ANALIZZARE I RISCHI DERIVANTI DAL TRATTAMENTO
- ANALIZZARE LE MISURE DI SICUREZZA ADEGUATE ADOTTATE DAL FORNITORE NELLO SPIRITO DELLA «PRIVACY BY DESIGN»
- DECIDERE IL CICLO DI VITA DEI DATI: PER QUANTO TEMPO SARANNO CONSERVATI E COME VERRANNO CANCELLATI
- ORGANIZZARE LA RACCOLTA DEL CONSENSO E DELLA DISTRIBUZIONE DELL'INFORMATIVA
- AUTORIZZARE LE PERSONE ALL'ESECUZIONE DELLA RACCOLTA E DELLA GESTIONE
- FORMARE LE PERSONE SULLE MISURE DI SICUREZZA DA ATTUARE E RISPETTARE
- TENUTA DEL «REGISTRO DEL TITOLARE»
- NOMINARE IL DPO (DATA PROTECTION OFFICER) PER I TRATTAMENTI CHE LO RICHIEDONO

ZUCCHETTI

PARTICOLARITA’

NELLA SOLUZIONE «CLOUD» IL GESTORE DEL SERVIZIO HA ACCESSO AD **UN ENORME VOLUME DI DATI** PERSONALI DEI CLIENTI

LE APPLICAZIONI CLOUD NON SEMPRE SONO EROGATE DA STRUTTURE PROPRIETARIE DEL PRODUTTORE, ANZI E’ SEMPRE PIU’ DIFFUSO L’AFFITTO DI **SPAZI IN DATA CENTER DI TERZE PARTI**

IL RISCHIO PERCEPITO DAL TITOLARE E’ PIU’ ELEVATO DI QUELLO CHE RISULTA DALL’ARCHITETTURA GESTITA DAL RESPONSABILE

IL PRODUTTORE DISPONE DI TUTTI I DATI DEI SUOI CLIENTI, DANDO COSI’ VITA AD UN «HONEYPOT» CHE PUO’ RISULTARE MOLTO **INTERESSANTE A TERZI CHE POTREBBERO ACCEDERVI ILLEGALMENTE**

UN «DATA BREACH» DI SOLI DATI DI UN SINGOLO TITOLARE **E’ MOLTO MENO PERICOLOSO** CHE UN «DATA BREACH» DI UNA GRANDE DATA CENTER

Che garanzie richiedere nei servizi erogati dai fornitori

Irrobustimento dell'applicazione rispetto ad attacchi ed errori	
Separazione dei dati	
Chiavi "mute"	• Nella scelta dei dati che vengono utilizzati per creare le chiavi primarie cercare di scegliere sempre dati che non identificano le persone.
Hash delle password	•Le applicazioni devono memorizzare le password degli utenti e questo archivio è immediatamente un "honey pot" per gli attaccanti. Il sistema ad oggi riconosciuto come robusto è mantenere un hash della password con algoritmi di hash crittografici
Password "at rest"	•Se l'applicazione deve comunicare con altri sistemi deve memorizzare password di accesso che inevitabilmente restano per molto tempo nel sistema. E' opportuno proteggerle con particolari accorgimenti.
Multitenancy	•Se l'applicazione prevede la possibilità di essere utilizzata da più utenti completamente scollegati tra loro, come avviene per molte applicazioni fornite in SaaS, la gestione più sicura è quella che prevede database separati per ogni titolare
Aggiornamento delle librerie	•Tutti i sistemi complessi vengono costruiti basandosi su mattoni di base acquisiti dall'esterno. Nella costruzione di applicazioni che trattano dati personali è estremamente importante che siano controllate le segnalazioni di sicurezza delle componenti utilizzate ed adottino le versioni sicure appena disponibili.
Distribuzione continua delle patch	
Aggiornamento continuo dei sistemi	
Penetration test e vulnerability assessment	
Sistema di qualità	
Rilevamento dei data breach	

ZUCCHETTI

ZUCCHETTI

Il software che crea successo