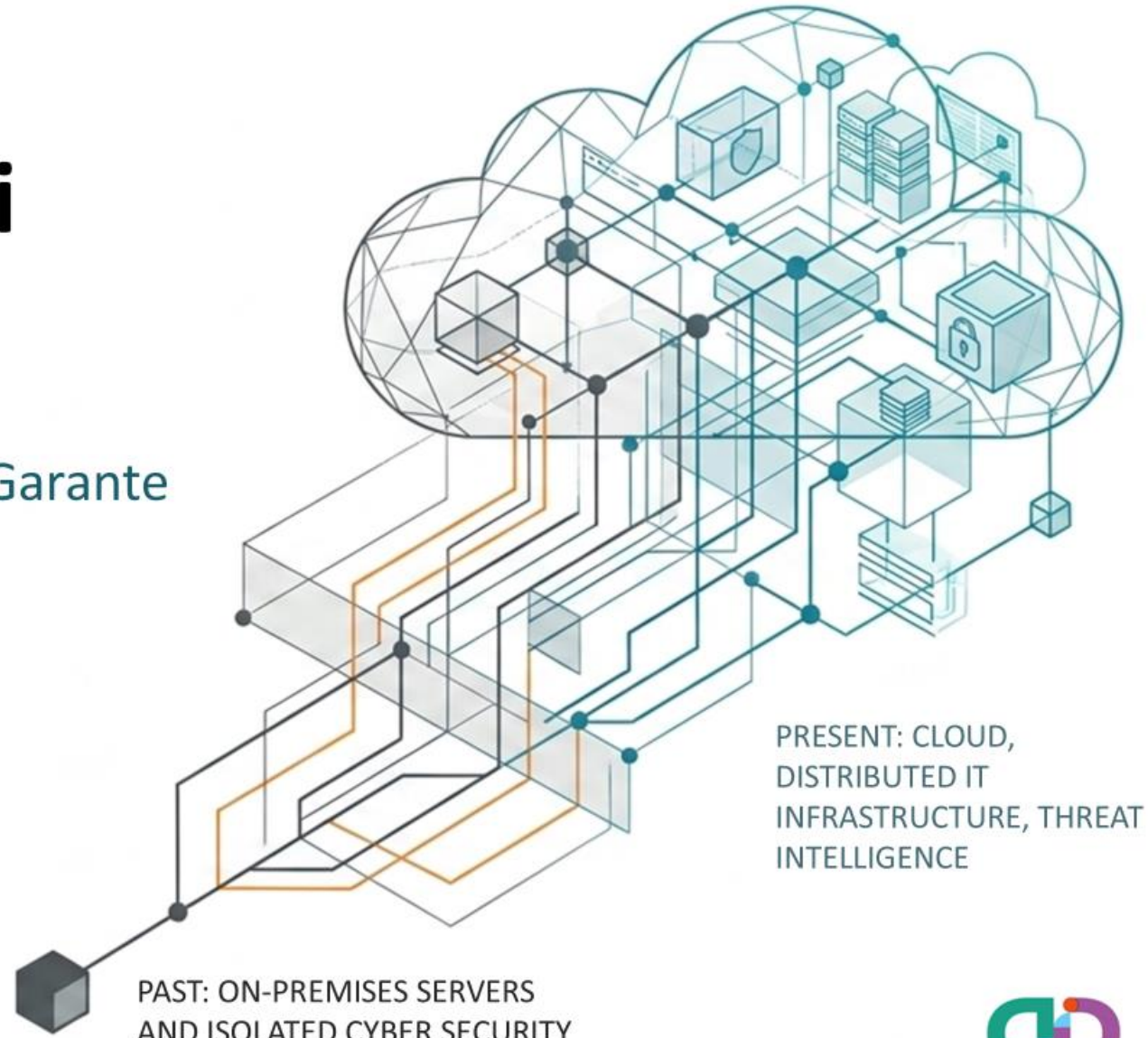
L’evoluzione dell’Amministratore di Sistema

Rileggere il Provvedimento dell’Autorità Garante
per una gestione efficace
della compliance digitale
tra modelli di governance dei dati
e gestione della cyber security
nell'era del cloud e di NIS 2



STUDIO LEGALE LISI

DIGITALAW

La metamorfosi del contesto di operatività degli Amministratori di Sistema

2008 - 2009:
Provvedimento del Garante sugli AdS e Allegato B

Manutenzione fisica, sistemi locali e perimetri isolati.

2016 - 2018:
GDPR, evoluzione degli asset e adeguatezza delle misure

Database complessi e reti aziendali interne.

Oggi:
NIS 2, threat intelligence e presidio di accountability multirischio

Infrastrutture distribuite, gestione del rischio e continuità operativa ISO 22301

La natura dell'AdS non è più solo operativa, ma fiduciaria. L'incarico comporta elevate criticità per la protezione dei dati, richiedendo requisiti tecnici, di esperienza e di affidabilità rigorosi.

Muta lo scenario, cambia l'interpretazione

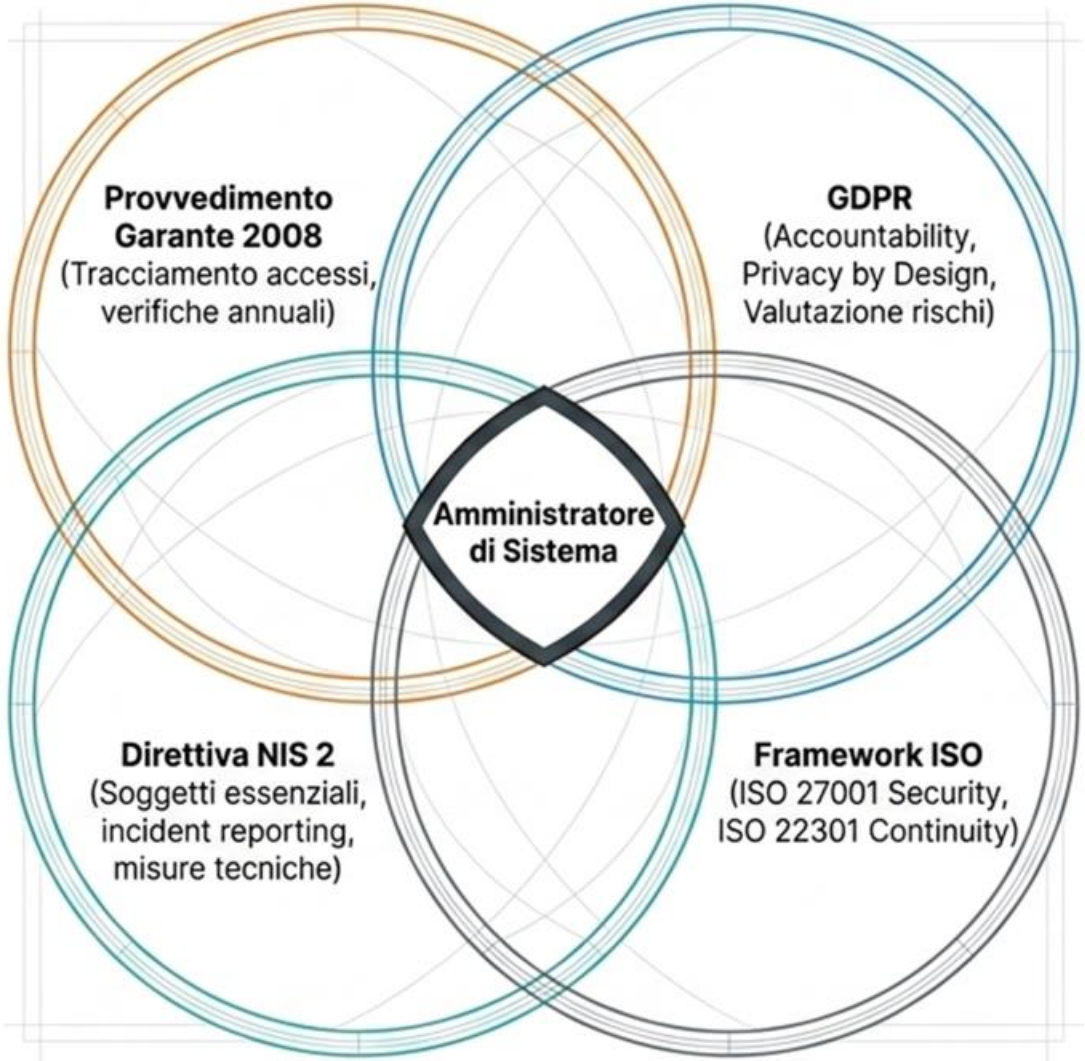
Le infrastrutture IT nelle organizzazioni del 2008

- Sistemi On-premise
- Perimetri fisici definiti
- Login su singolo server
- Focus sulle Misure Minime di base

Le infrastrutture IT nelle organizzazioni oggi

- Infrastrutture Cloud / IaaS
- Architetture distribuite e senza perimetro (Zero Trust)
- Identity & Access Management (IAM)
- Misure di sicurezza proporzionate al rischio (GDPR)

L’Amministratore di Sistema come ruolo chiave per la compliance digitale



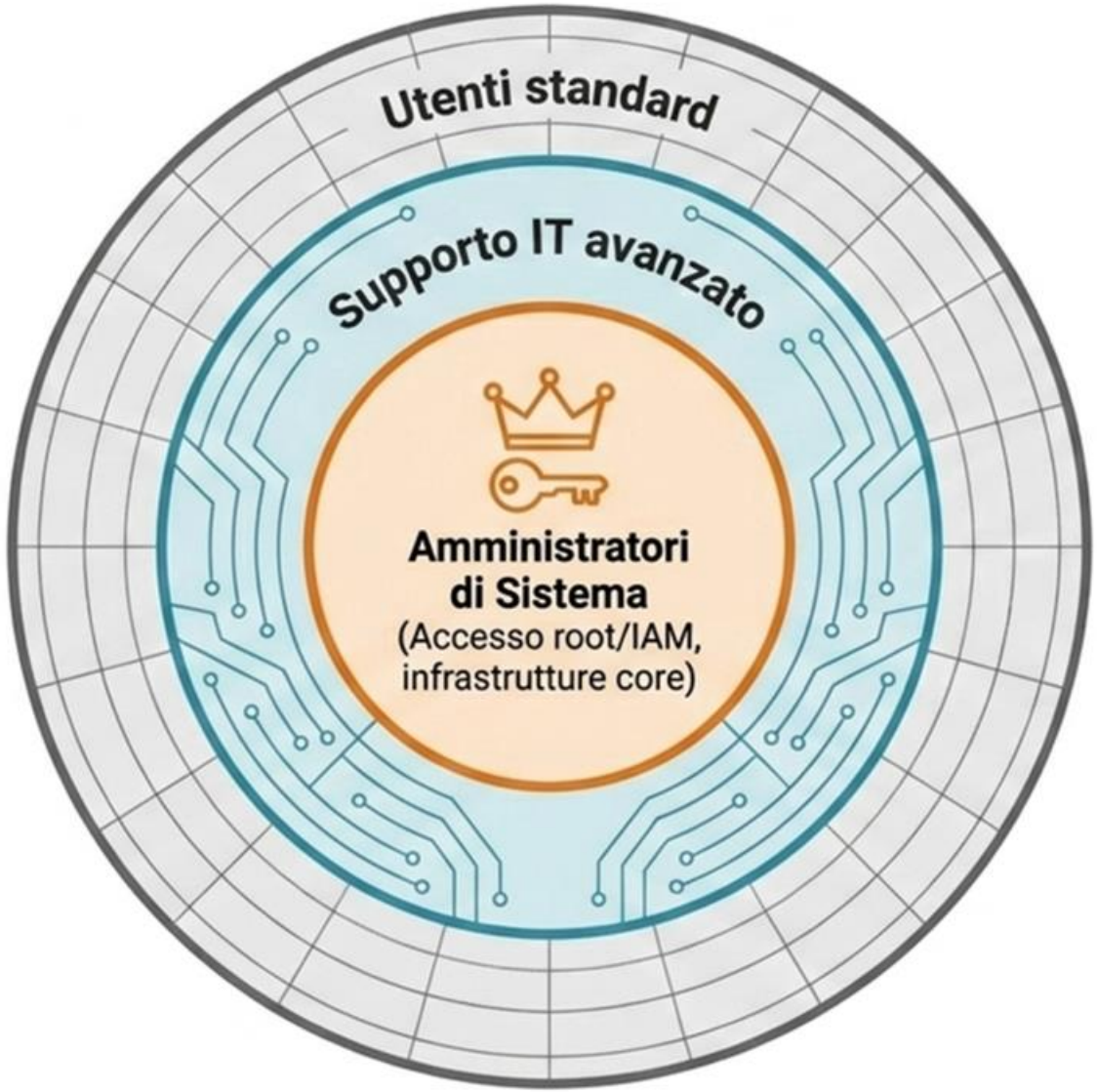
Chi deve essere individuato oggi come AdS?

Principali criteri di orientamento in base all'operatività

RISULTATO: Se la risposta è Sì, la figura richiede nomina formale, log degli accessi e audit annuale.

N.B.: sono esclusi i soggetti che effettuano attività puramente occasionali

Come distinguere il ruolo di AdS da altri ruoli IT?



- Abbandonare l'etichetta generica di informatico.

- Mappare chiunque abbia concreta **capacità di azione intenzionale o fortuita** sui sistemi critici.

- Assicurare che il Registro dei Trattamenti dialoghi con le policy di security (es. livelli di rischio NIS 2: Essenziali vs. Importanti).

Focus: punti di attenzione per le organizzazioni

Checklist operativa per l'individuazione e la nomina degli AdS

INDIVIDUAZIONE

- Mappare TUTTE le figure con accesso privilegiato (root, admin, sudo, IAM admin) — inclusi MSP (Managed Service Provider), consulenti IT, sviluppatori con accesso prod
- Non fermarsi al titolo: il “DevOps Engineer” (che unisce lo sviluppo software – Dev - e le operazioni IT – Ops - per automatizzare e velocizzare il rilascio di applicazioni) o il “Cloud Architect” se trattano dati personali sono AdS
- Nei gruppi societari: l'AdS di shared services IT è AdS per ogni società del gruppo che beneficia dei sistemi

NOMINA FORMALE

- Nominare formalmente e singolarmente ogni persona fisica: non basta la clausola generica nel contratto con il partner IT o il MSP
- L'atto di nomina deve elencare analiticamente i sistemi/ambiti (es. “Azure subscription ID xxx, AWS account yyy, server ESXi zzz”)
- Per gli AdS in outsourcing: conservare gli estremi identificativi delle persone fisiche (nome, cognome, ruolo)
- Aggiornare la nomina ad ogni cambio di personale presso il partner IT

LOG & AUDIT

- Verificare che il SIEM/log collector copra TUTTI i sistemi su cui l'AdS opera (inclusi cloud, VPN, DBMS)
- Garantire inalterabilità: log forwarding in append-only su storage dedicato o SIEM con write-once
- Conservazione minima 6 mesi: inserire SLA nel contratto con partner IT, MSP o fornitore cloud
- Documentare la revisione annuale dei log come parte del processo di verifica dell'operato AdS

NIS 2 / SICUREZZA

- Per soggetti NIS2: integrare nomina AdS con policy PAM (Privileged Access Management), MFA obbligatoria e session recording
- Verificare che il contratto con il partner o fornitore IT preveda obblighi NIS2 sulla supply chain (art. 21 Direttiva NIS 2)
- In caso di incidente: i log AdS sono prova; la mancanza di nomina e log aggrava la gestione delle conseguenze dell’incidente e impedisce di risalire alle reali responsabilità
- Il CISO/SOC team che accede a sistemi con dati personali in modalità privilegiata è AdS: occorre nominarlo

Il Provvedimento del Garante del 2008 è ancora in vigore, ma non va applicato come mero adempimento formale, bensì sulla base di un approccio alla compliance che sia «su misura» dell'organizzazione e che valorizzi le attività effettivamente svolte, i sistemi interessati e gli assetti contrattuali con i partner IT.

DIGITALAW

STUDIO LEGALE LISI

La presente infografica, a cura dell'Avv. Sarah Ungaro, è un contenuto riservato in anteprima agli iscritti della Newsletter dello Studio legale Lisi del 29 aprile 2026