rethinking the future together

Alessandro Gaspari
Data Center Specialist
alessandro.gaspari@testspa.com

L'adeguamento al GDPR

General Data Protection Regulation (GDPR) - (UE) 2016/679

Regolamento europeo in materia di protezione dei dati personali

INDICE

CONCETTI DI BASE

GDPR

- Il **25 maggio 2018** entrerà in vigore il nuovo Regolamento europeo in materia di trattamento dati personali (GDPR) – Regolamento europeo (UE) 2016/679.
- Il sistema sanzionatorio predisposto punisce sempre e tutto anche le inosservanze minime.
- L'entità delle sanzioni possono arrivare fino 20 milioni di Euro o al 4% del fatturato annuale.

ALCUNE NOVITA' DEL GDPR CHE IMPATTANO L'ICT

- **Privacy by Design**, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema.
- **Accountability**, ovvero resposabilizzazione attraverso l'analisi dei rischi ed eventuale valutazione d'impatto.
- Obbligo di communicate i casi di violazione dei dati ("**data breach**").
- **Portabilità** dei dati.
- **Diritto all'oblio**.

MISURE MINIME?

NON ESISTONO PIU’ LE MISURE MINIME PRESENTI SUL CODICE PRIVACY

SICUREZZA DEL TRATTAMENTO

TITOLARE e RESPONSABILI

RESPONSABILITA' (accountability)

Tenuto conto di: **natura, ambito, contesto, finalità, rischi e costi di attuazione**

Mettono in atto **misure tecniche e organizzative** per **garantire** un **livello di sicurezza adeguato al rischio** e **dimostrare** che il trattamento è stato effettuato conformemente al regolamento

ANALISI DEI RISCHI

TITOLARE e RESPONSABILI

ANALISI DEI RISCHI
(art. 24)

REGISTRO DEI TRATTAMENTI
(art. 30)

MISURE TECNICHE ADEGUATE PER MITIGARE IL RISCHIO

a. **Pseudonimizzazione** e **cifratura** dei dai personali.

b. Capacità di assicurare la continua **riservatezza**, **integrità**, **disponibilità e resilienza dei sistemi e dei servizi** che trattano i dati personali

c. **Capacità di ripristinare tempestivamente la disponibilità** e l'accesso dei dati in caso di incidente fisico o tecnico;

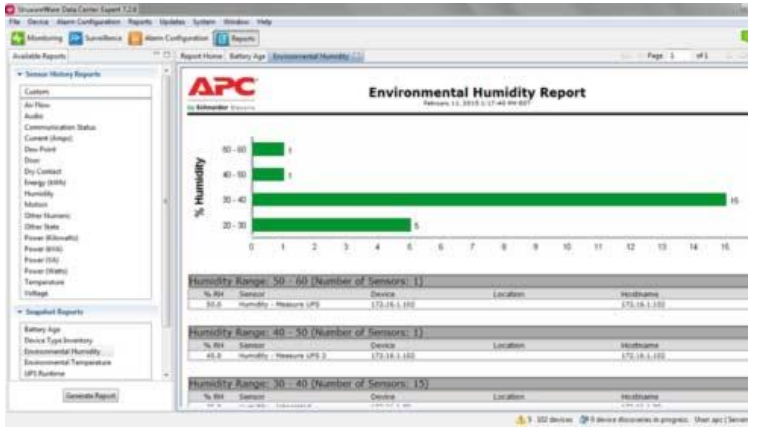
d. Procedura per **provare**, **verificare** e **valutare** regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

RELAZIONE TRA MISURE TECNICHE E ICT

DISPONIBILITA' E RESILIENZA	Caratteristiche dei CED/sistemi IT (UPS, Condizionamento, Antincendio, Controllo accessi, Hosts, Storage, ecc.).
CAPACITA' DI RIPRISTINARE	Backup e Disaster Recovery.
PSEUDONIMIZZAZIONE	Cifratura dei volumi (Server, Desktop, Laptop), Pseudonimizzazione applicazioni con specifici rischi sulla sicurezza delle persone.
PROCEDURA PER PROVARE E VERIFICARE	Analisi dei Rischi, Registro trattamenti, Documentazione Privacy, Audit interno. Firewall, GPO, Log management, Vulnerability Scan, ecc..

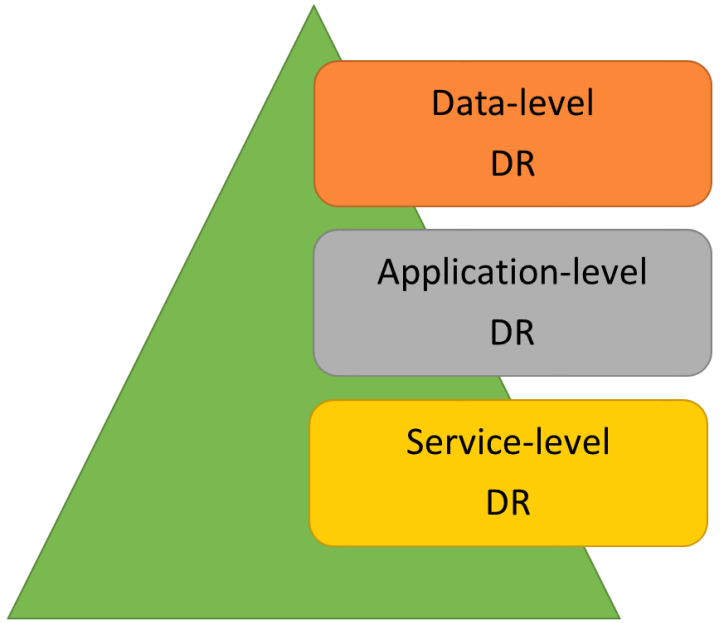
AMBITO - DATA CENTER

- Sistemi per continuità operativa
  - UPS, GE
  - Topologie N+1, 2N
- Sistemi di sicurezza
  - Controllo accessi, antiintrusione
  - TVCC
  - Sistemi rilevazione e spegnimento incendi
  - Sistemi di monitoraggio



AMBITO - SISTEMI

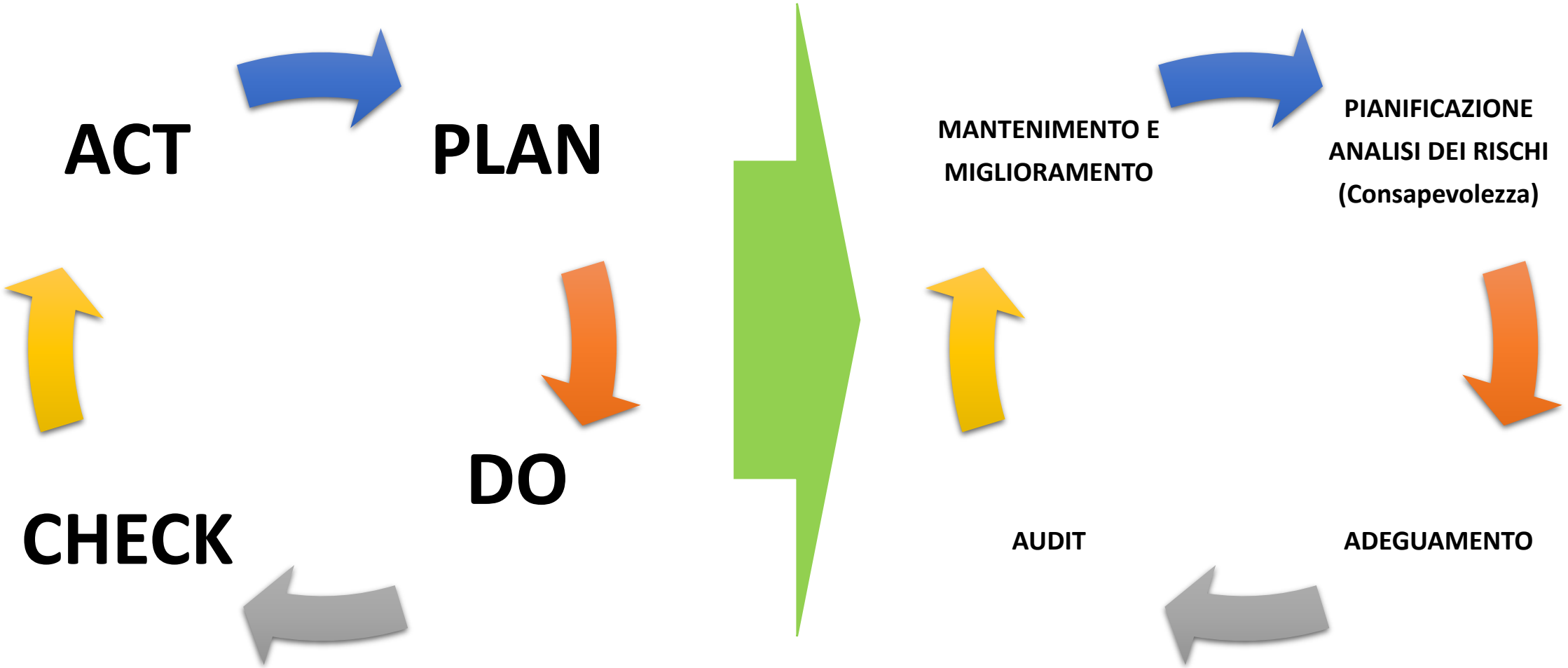
- Server
  - Cluster Virtualization
  - Iperconvergenza
- Storage
  - Servizi Metro Cluster o Replica S/A
  - Iperconvergenza
- Backup & DR
  - Backup e gestione del ciclo di vita del dato
  - Disaster Recovery
- Servizi Cloud
  - Exit Strategy
  - Politiche di gestione dei dati
  - Service Level Agreement



Livelli Disaster Recovery

PROCESSO DI ADEGUAMENTO

IL PROCESSO DI ADEGUAMENTO



FASI DI ADEGUAMENTO

Verifica Compliance (AUDIT)

- Raccolta di tutte le informazioni, analisi e valutazione della documentazione in uso.
- Raccolta informazioni dei trattamenti in uso.

Consapevolezza

- Analisi dei rischi connessi ai trattamenti. Eventuale “analisi di impatto” (non obbligatorio).
- Individuazione degli asset aziendali e delle piattaforme esterne.
- Registro dei trattamenti (titolare e responsabile) con indicazione delle finalità e durata del trattamento , della categoria dei dati personali, di eventuali destinatari.
- Individuazione dei responsabili del trattamento.
- Individuazione dei ruoli e delle responsabilità degli incaricati al trattamento.

FASI DI ADEGUAMENTO

Adeguamento

- Modifica documentazione (es. Informative) per allinearla alle nuove prescrizioni.
- Definizione e implementazione delle politiche di sicurezza vista l'analisi dei rischi precedente.
- Formazione.

Audit

- Monitoraggio del Sistema mediante Audit Interno.

METODI E STRUMENTI UTILI

SISTEMI DI GESTIONE E STANDARD VOLONTARI UTILI

Sistemi di Gestione

- ISO 9001 Sistema gestione della qualità
- ISO 27001 Sistema gestione della sicurezza dell'informazione e in generale tutte le ISO della serie 27xxx
- ISO 22313:2015 Sistemi di gestione per la continuità operativa.

Infrastrutture

- TIA-942
- Uptime Institute

CLASSIFICAZIONE CED PA / TIA-942 – RATING 3

a. Lo standard di riferimento è la TIA-942 «Telecommunications Infrastructure Standard for Data Centers» (TIA - Telecommunication Industry Association).
b. Il livello di riferimento è il Rating 3.

Concurrent Maintainable; il data center può sopportare qualsiasi tipo di manutenzione (programmata/non programmata) senza interruzione dei servizi con supporto 24x7 alle operazioni.

CERTIFICAZIONE SITEMA DI GESTIONE PRIVACY

a. Al momento l'unico sistema di gestione per la privacy standardizzato è il BS10012:2017 (British Standard).
b. Le certificazioni e i codici deontologici richiamati nella sezione 5, art.40-art.43 sono ancora in fase di definizione.
c. Un utile punto di partenza per definire un Sistema di gestione privacy o MOP (Modello Organizzativo Privacy) potrebbe essere quello di utilizzare la ISO 9001 sostituendo il termine "qualità" con ."privacy" e "cliente" con "interessato"

GRAZIE

www.testspa.com