La Cybersicurezza come Priorità Strategica

Il modello collaborativo toscano

giovedì 18 dicembre 2025

NB: slide prodotte da un essere umano, immagini generate con l'IA

Backup e restore

Perché il backup è vitale (non solo importante)?

… per rispondere celermente a situazioni come queste:

01

Servizi digitali fermi

Anagrafe, stato civile, edilizia, tributi, autorizzazioni, Rete Civica, …

02

Dati digitali criptati e inaccessibili

Bilancio, personale, protocollo informatico, file e cartelle condivise, sistema interno di autenticaione

03

Richiesta di riscatto

Che in ogni caso non va mai pagato

Webinar del 4 dicembre ANCI per la Comunità di Pratica sulla cybersicurezza

Perché il backup è vitale (non solo importante)?

… e poter recuperare i dati (restore) a fronte delle cause più diverse:

01

Problemi tecnici

Corruzione dati a causa di apparati server o storage che si rompono, sistemi con bug, software che vanno in crash, aggiornamenti falliti, …

02

Errore umano

Cancellazione accidentale di dati, sovrascrittura errata di file e documenti, configurazioni sbagliate, …

03

Disastri ed eventi esterni

Allagamenti, incendi, terremoti, furto o smarrimento di dispositivi, interruzioni elettriche prolungate (blackout), …

04

Compromissioni di cybersicurezza

Malware o virus che blocca i sistemi, accessi non autorizzati che alterano i dati, attacchi ransomware, …

ad oggi sono le principali cause

Ma quando si è iniziato a parlare di backup?

1

Antichità
Esiste il concetto di avere copie di informazioni importanti usando tavole di argilla e papiri

2

Albori dell'informatica (1950-70)
Copia di sicurezza per proteggere i dati su schede perforate e nastri, nasce il concetto di "*backup*"

3

Diffusione dell'informatica (1970-'90)
Mainframe e avvento dei personal computer, il backup diventa pratica IT fondamentale con procedure regolari e varie tipologie di supporti

4

Era modarna (2000-?)
Evoluzione delle tecnologie: sistemi automatici, server e software dedicati, off-site, strategie incrementali e differenziali, cloud backup, DR e il backup di ciascun dispositivo personale...

Quindi ormai è già tutto definito e standardizzato?

Certamente il backup NON è un "*optional*"...

- **Obbligo normativo**: GDPR e *accountability*, rispetto delle Misure Minime ICT per la PA per la capacità di ripristino e, più di recente, gli adempimenti per la NIS e la NIS2 (D.lgs. n.138/2024) per i soggetti che rientrano nel perimetro di applicazione

- **Responsabilità amministrativa**: garantire la continuità dei servizi erogati

- **Tutela patrimonio pubblico**: assicurare la salvaguardia di dati e dei documenti digitali della propria Amministrazione

Tutti facciamo backup, ma saranno fatti "bene"?

Altrimenti potrebbero esserci problemi proprio quando servono! Vediamo un veloce elenco degli errori più comuni:

01

Backup solo on-site

Stessa sede e/o datacenter dei dati da proteggere: se perdi quella sala perdi anche i salvataggi fatti

02

Backup accessibile su rete

La soluzione di backup è collegata alla stessa rete che ospita i sistemi protetti: un cyberattacco (ransomware) può raggiungerlo e cifrare i salvataggi

03

Backup con frequenza inadeguata

L'ultimo backup disponibile risale a una settimana fa e potresti perdere diversi giorni di lavoro

04

Backup senza cifratura

Dati salvati in chiaro: si rischiano delle violazioni normative e possivili sanzioni nel caso di esfiltrazione o accesso non autorizzato agli stessi

05

Backup ok, restore mai testato

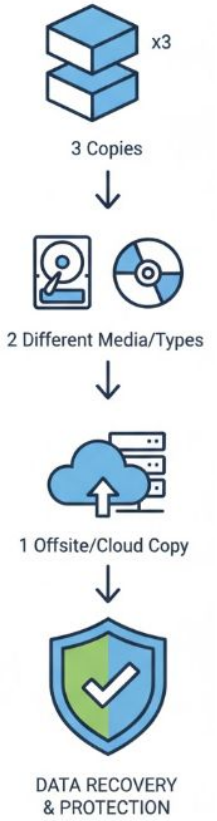
La soluzione di backup è perfetta, ma non si trova il tempo dei test di restore: rischio concreto di non poter recuperare i dati quando serviranno davvero

06

Backup/restore ok, no documentazione

A livello tecnologico tutto ok e presidiato: in caso di emergenza o in assenza di figure chiave, si rischia poi di non avere le informazioni necessarie a poter operare

Alcuni concetti di backup su cui si è basato il lavoro del gruppo



Adottare una "strategia 3-2-1", abbastanza lineare ed efficace:

3. **Ovvero tre copie dei dati**: dati originali, backup e relativa copia

2. **Ovvero due supporti diversi:** papiri e tavole di argilla, disco locale e cloud, ecc.
1. **Ovvero una copia fuori sede:** in altra località fisica (altra sede o cloud)

\+ **Plus con copia air-gapped:** avere una copia isolata dalla rete di produzione

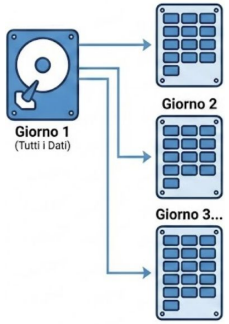
Un esempio "sostenibile" da contrattualizzare per comune medio-piccolo:

- dati nei server di produzione in datacenter qualificati
- backup su storage stesso datacenter (on-site e online)
- copia in diverso datacenter o cloud qualificato ACN (off-site e online)
- (plus) replica cloud su rete isolata (air-gapped)

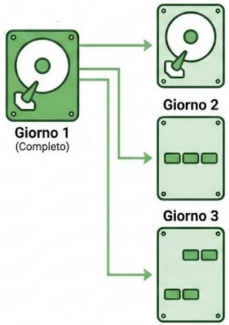
Alcuni concetti di backup su cui si è basato il lavoro del gruppo

Considerazioni veloci su policy e frequenze dei backup:

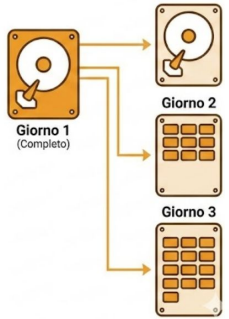
1. **Completo (full):**
   - Salvare sempre tutto
   - assicurando ripristino veloce
   - ma occupando più spazio e richiedendo più tempo



2. **Incrementale (incremental):**
   - Salvare solo ciò che è stato modificato dall'ultimo backup
   - assicurando velocità di salvataggio e minor occupazione spazio
   - ma richiedendo più tempo per il ripristino



3. **Differenziale (differential):**
   - Salvare tutto ciò che è stato modificato dall'ultimo backup completo
   - con prestazioni intermedie su durata, spazio e velocità di ripristino



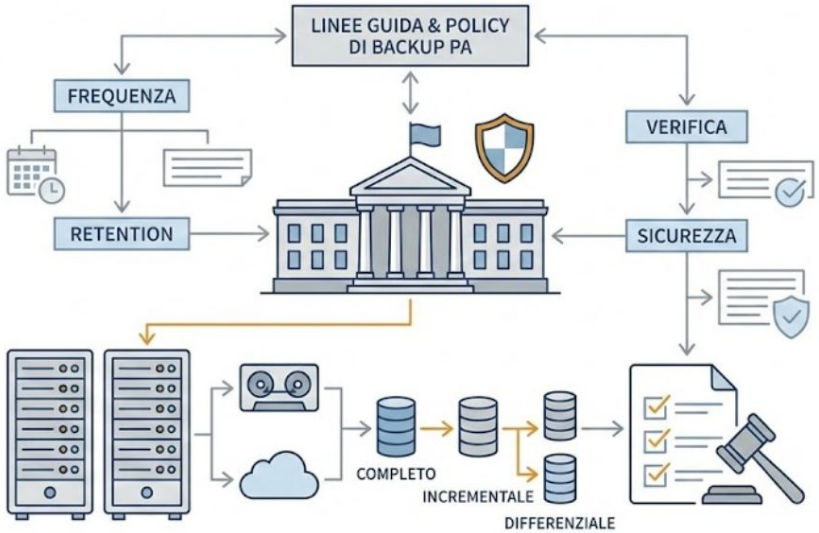
Un esempio "sostenibile" per comune medio-piccolo:

- Backup completo di domenica (c'è più tempo per completarlo)
- Backup incrementale/differenziale notturno da lunedì a sabato
- Occupazione spazio ottimizzata con copertura sulle 24 ore

Cosa è stato prodotto dal gruppo di lavoro in tale ambito?

Un documento contenente le Linee Guida di Backup & Restore:

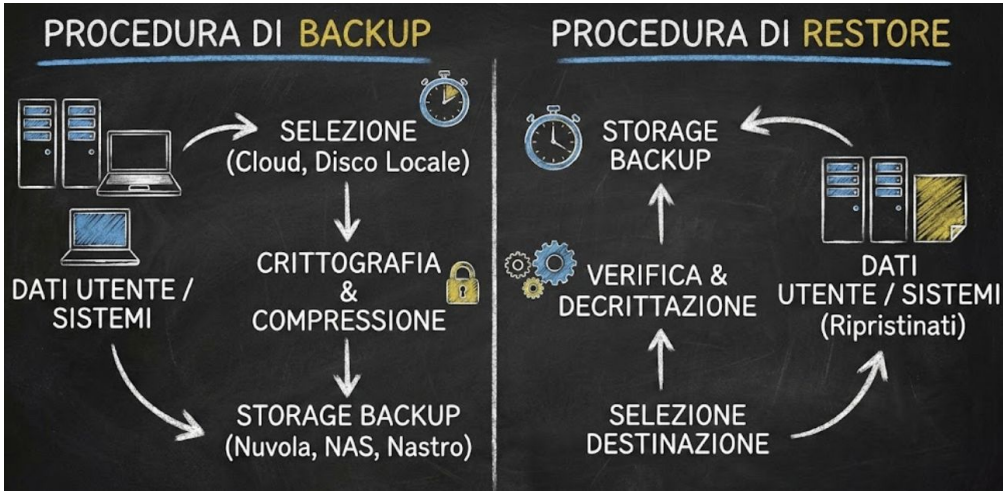
Linee Guida Backup & Restore



Questa documentazione nasce come evoluzione di quella prodotta in un progetto multi-ente finanziato con PNRR, avviso 3/2022 di ACN. Nelle linee guida vengono trattati diversi ambiti con lo scopo di fornire raccomandazioni, policy e indicazioni di riferimento per definire poi la procedura per gestire i backup del proprio Ente.

Cosa è stato prodotto dal gruppo di lavoro in tale ambito?

Un template "compilabile" per la propria procedura di Backup & Restore:



Template - Procedura di Backup & Restore

Il template contiene una struttura e un'impostazione generale che ciascun Ente può poi compilare e completare, adattandolo a quanto presente nella propria realtà (obiettivi, ambito, infrastruttura, policy, modalità, test, ripristino e aggiornamento).

Conclusioni ...

Perché usare la documentazione prodotta (e completarla internamente!):

- Come guida e punto di riferimento (anche rispetto a quanto già esistente)
- Poter conseguire progressivamente una conformità normativa
- Richiamo alle raccomandazioni e alle migliori pratiche di settore
- Attenzione nel garantire soluzioni applicabili e un approccio concreto
- Scalabilità di quanto prodotto, partendo da comuni piccoli a medie realtà
- Per confrontarsi con il proprio fornitore in fase di contrattualizzazione

... e i ringraziamenti!