Prova 1

1) In un'architettura a microservizi containerizzata e orchestrata, come progetterebbe la comunicazione tra servizi, la segmentazione della rete e la gestione della sicurezza, garantendo al contempo scalabilità e resilienza?

2) Nel processo di reingegnerizzazione di un applicativo web legacy, sviluppato internamente e privo di adeguata documentazione, come affronterebbe il bilanciamento tra usabilità e requisiti di sicurezza derivanti dalle linee guida AgID e dalla direttiva NIS2? Descriva l'approccio tecnico che adotterebbe per adeguare il sistema ai requisiti normativi senza compromettere la continuità e l'efficacia del servizio.

3) In un'applicazione PHP in produzione che presenta degrado prestazionale e comportamenti intermittenti sotto carico, come strutturerebbe l'analisi e l'intervento a livello di codice e configurazione? Descriva gli strumenti che utilizzerebbe e le modifiche concrete che apporterebbe.

4) Traduca e commenti:

Regulations for the Use of SISSA Storage Space

Introduction

In the context of European research projects, especially those funded under Horizon Europe and similar frameworks, the FAIR principles — Findable, Accessible, Interoperable, and Reusable—are essential for ensuring that research data is managed responsibly and shared effectively. These principles not only enhance the transparency, reproducibility, and impact of scientific research but are also increasingly required by funding agencies.

Purchasing storage involves acquisition costs, operational costs, and costs related to the space occupied in the data room. To optimize these costs, SISSA has implemented high-capacity, expandable storage, through which space can be allocated to each research group upon request.

The School has decided to establish a central archive to support Principal Investigators (PIs). This strategy aims to streamline data management and optimize resources by discontinuing the acquisition of NAS or other types of storage for individual groups or projects.

Prova 2

1) In un'architettura a microservizi distribuita con database separati per servizio, come garantirebbe coerenza dei dati, gestione delle transazioni e resilienza ai guasti, considerando anche aspetti di networking e sicurezza?

2) Nel contesto del rifacimento di un applicativo web esistente, privo di documentazione tecnica e sviluppato da un collega non più in servizio, come gestirebbe un possibile conflitto tra le esigenze funzionali degli utenti (es. docenti o studenti) e i vincoli di sicurezza imposti dalle normative AgID e NIS2? Quale approccio metodologico e tecnico adotterebbe per garantire la messa in sicurezza dell'applicativo?

3) In un'applicazione PHP legacy in produzione che deve essere aggiornata a una versione recente di PHP (es. 8.x) garantendo continuità del servizio, come pianificherebbe e realizzerebbe l'intervento a livello di codice, dipendenze, configurazione e ambiente? Descriva le verifiche, i test e le misure di rollback che adotterebbe.

4) Traduca e commenti:

NIS2 Directive: securing network and information systems

The NIS2 Directive establishes a unified legal framework to uphold cybersecurity in 18 critical sectors across the EU. It also calls on Member States to define national cybersecurity strategies and collaborate with the EU for cross-border reaction and enforcement.

The directive mandates that each Member State adopt a national cybersecurity strategy, which includes policies for supply chain security, vulnerability management, and cybersecurity education and awareness. Member States must also establish and regularly update a list of operators of essential services, ensuring these entities comply with the directive's requirements.

As a rule, medium-sized and large entities in these critical sectors, will have to take appropriate cybersecurity risk-management measures and notify relevant national authorities of significant incidents. These are incidents that could cause significant disruption or damage.