Concorso pubblico per esami per 1 posto Area delle Elevate Professionalità - settore professionale tecnico-informatico per la Direzione Informatica e Tecnologie (cod. 2026epta004)

Bandito con D.D. n. 4352/2026 Prot n. 177914 del 29/04/2026, pubblicato sul Portale Unico del Reclutamento InPA e sul sito web di Ateneo in data 04/05/2026

II PROVA SCRITTA – 29 luglio 2026

PROVA PROGETTUALE

Progettazione dell'evoluzione, della sicurezza e della resilienza dell'ecosistema digitale di un Ateneo

Durata della prova: 2 ore

Traccia 1

PREMESSE

Contesto di riferimento

Un Ateneo pubblico di grandi dimensioni supporta le proprie attività didattiche, di ricerca e amministrativogestionali mediante un ecosistema ICT articolato ed eterogeneo.

L'attuale architettura comprende:

- due data center di Ateneo, nei quali sono ospitati server fisici, infrastrutture virtualizzate, sistemi di storage e database enterprise;

- infrastrutture cloud pubbliche e private utilizzate secondo modelli IaaS e PaaS;

- servizi SaaS, tra cui Microsoft 365, piattaforme per la collaborazione, applicazioni amministrative e servizi specialistici;

- un sistema centralizzato di Identity and Access Management, integrato con Active Directory, servizi di Single Sign-On e federazioni di identità;

- database Oracle, Microsoft SQL Server e PostgreSQL, gestiti da gruppi tecnici differenti;

- piattaforme per la didattica digitale e laboratori informatici utilizzati dagli studenti;

- infrastrutture HPC e cluster GPU a supporto della ricerca scientifica, della data science e delle applicazioni di intelligenza artificiale;

- sistemi di backup e replica differenziati, non sempre governati secondo standard omogenei;

- strumenti di monitoraggio, logging e sicurezza gestiti da più unità organizzative e fornitori esterni.

Nel corso degli anni i servizi sono stati sviluppati o acquisiti in modo progressivo, con conseguente eterogeneità delle tecnologie, delle modalità di gestione e dei livelli di servizio.

L'Ateneo è classificato come soggetto importante ai sensi della normativa NIS2 e intende rafforzare il proprio sistema di gestione della sicurezza, perseguendo inoltre, per il perimetro della Direzione ICT, un progressivo allineamento alla norma ISO/IEC 27001.

Problematiche rilevate

Un'analisi preliminare ha evidenziato le seguenti criticità:

- assenza di una classificazione unitaria dei servizi in base a criticità, requisiti di disponibilità e sensibilità dei dati trattati;

- dipendenze tra sistemi on premises, cloud e SaaS non completamente documentate;

- procedure di provisioning e deprovisioning delle utenze non uniformi, in particolare per collaboratori, ospiti, ricercatori e soggetti esterni;

- presenza di account amministrativi permanenti e privilegi non sempre sottoposti a revisione periodica;

- strumenti di monitoraggio, logging e rilevazione degli incidenti non pienamente integrati;

- strategie di backup, replica e Disaster Recovery differenziate tra i diversi servizi;

- test di ripristino e continuità operativa effettuati in modo non sistematico;

- utilizzo crescente di servizi cloud e SaaS, con rischi di dipendenza tecnologica e contrattuale dai fornitori;

- crescita della domanda di risorse HPC, GPU e piattaforme per applicazioni di intelligenza artificiale;

- frammentazione delle responsabilità tra unità ICT centrali, strutture dipartimentali, responsabili applicativi e fornitori esterni.

Evento scatenante: compromissione cyber dell'infrastruttura ibrida e dei sistemi di backup

L'Ateneo ha recentemente subito un incidente di sicurezza informatica che ha interessato una parte significativa della propria infrastruttura digitale.

L'incidente ha avuto origine dalla compromissione di un account amministrativo utilizzato per la gestione di sistemi virtualizzati. Le credenziali dell'account, non protetto mediante autenticazione multifattore e caratterizzato da privilegi estesi, sono state utilizzate per accedere a diversi ambienti on premises e cloud.

L'attaccante ha successivamente:

- acquisito privilegi elevati su alcuni sistemi;

- compromesso parte dell'infrastruttura Active Directory;

- cifrato server virtuali utilizzati da servizi amministrativi e didattici;

- cancellato o reso indisponibili alcune copie di backup collegate direttamente all'infrastruttura di produzione;

- tentato di accedere a database contenenti dati personali e informazioni relative alle attività di ricerca;

- utilizzato account tecnici per propagarsi verso ulteriori componenti dell'infrastruttura;

- interrotto per circa ventiquattro ore alcuni servizi essenziali.

L'impatto è stato parzialmente contenuto grazie all'intervento dei gruppi tecnici, ma il ripristino dei servizi è risultato complesso e non coordinato. Per alcuni sistemi non è stato possibile determinare immediatamente se i dati fossero stati soltanto cifrati oppure anche esfiltrati.

L'incidente ha evidenziato:

- un'insufficiente segmentazione tra gli ambienti infrastrutturali;

- la presenza di account privilegiati permanenti e non adeguatamente monitorati;

- l'assenza di un modello uniforme di autenticazione forte e Privileged Access Management;

- la difficoltà di correlare tempestivamente i log provenienti da sistemi on premises, cloud e SaaS;

- la mancanza di un inventario completo degli asset, degli account tecnici e delle dipendenze tra i servizi;

- l'inadeguata segregazione delle infrastrutture di backup rispetto agli ambienti di produzione;

- l'assenza, per alcuni servizi, di copie immutabili, offline o logicamente isolate;

- la limitata disponibilità di procedure di ripristino documentate e verificate;

- l'incertezza nella ripartizione delle responsabilità tra gruppi infrastrutturali, responsabili applicativi, strutture dipartimentali e fornitori;

- criticità nel coordinamento tra risposta tecnica all'incidente, gestione della crisi, comunicazione istituzionale e adempimenti normativi.

Assegnazione progetto strategico

A seguito dell'evento, la Direzione Generale dell'Ateneo ha chiesto la predisposizione di un progetto organico di evoluzione dell'ecosistema ICT, da realizzare nell'arco di tre anni e finalizzato a:

- migliorare la resilienza, la sicurezza e la continuità dei servizi;

- razionalizzare l'architettura e le modalità di gestione degli ambienti on premises e in cloud;

- rafforzare il governo delle identità, dei dati, delle infrastrutture e dei fornitori;

- definire responsabilità, processi operativi e livelli di servizio coerenti con la criticità dei sistemi;

- assicurare sostenibilità tecnologica, economica e organizzativa, limitando i rischi di dipendenza da singoli fornitori o tecnologie.

Il progetto dovrà consentire non soltanto di rimuovere le vulnerabilità che hanno favorito l'incidente, ma anche di definire un modello strutturato di prevenzione, rilevazione, risposta e ripristino applicabile all'intero ecosistema digitale di Ateneo tenendo conto delle esigenze delle attività didattiche, amministrativo-gestionali e di ricerca.

Vincoli

La proposta dovrà tenere conto dei seguenti vincoli:

- necessità di garantire la continuità dei servizi durante la trasformazione;

- presenza di sistemi legacy e di contratti pluriennali non immediatamente modificabili;

- disponibilità limitata di risorse economiche e competenze specialistiche;

- distribuzione delle responsabilità tra strutture ICT centrali, dipartimenti, responsabili applicativi e fornitori;

- rispetto degli obblighi normativi applicabili, con particolare riferimento alla sicurezza informatica, alla protezione dei dati e alla normativa NIS2;

- necessità di preservare l'autonomia della ricerca, nel rispetto di requisiti comuni di sicurezza e governance.

Il candidato potrà formulare ulteriori ipotesi, purché siano esplicitate e coerenti con il contesto.

RICHIESTA

Il candidato, assumendo il ruolo di responsabile del progetto di cui alle PREMESSE, elabori una proposta di intervento articolata nelle seguenti sezioni:

1. Analisi e priorità

Individuazione dei principali requisiti, vincoli, rischi e dipendenze emersi dal caso, con indicazione delle priorità di intervento.

2. Soluzione tecnico-organizzativa

Descrizione dell'architettura e del modello operativo proposti, evidenziando:

- le principali scelte relative a infrastrutture on premises e in cloud;

- le misure di sicurezza, resilienza e protezione dei dati;

- le modalità di gestione delle identità, degli accessi e dei sistemi critici;

- il modello di governance e la ripartizione delle responsabilità.

La proposta dovrà approfondire gli aspetti maggiormente rilevanti rispetto all'evento di riferimento. Non è richiesta una trattazione analitica di tutte le tecnologie e di tutti i processi presenti nel contesto.

3. Piano di attuazione

Articolazione del programma in un numero limitato di fasi, distinguendo almeno:

- interventi urgenti;

- interventi di consolidamento;

- interventi strutturali.

Per ciascuna fase dovranno essere indicati i principali risultati attesi, le dipendenze e le responsabilità.

4. Verifica dei risultati

Individuazione di un insieme essenziale di indicatori utili a misurare l'efficacia degli interventi, con particolare riferimento a disponibilità, sicurezza, capacità di ripristino, qualità del servizio e avanzamento del programma.

Indicazioni per lo svolgimento

La proposta dovrà avere carattere progettuale e non meramente descrittivo.

Non è richiesto:

- il dimensionamento analitico delle infrastrutture;

- il calcolo dettagliato dei costi;

- il riferimento obbligatorio a specifici prodotti commerciali;

- lo sviluppo completo di procedure operative o documenti di conformità.

Le soluzioni proposte dovranno essere motivate in relazione ai requisiti, ai rischi e ai vincoli individuati.

PROVA PROGETTUALE

Progettazione dell'evoluzione, della sicurezza e della resilienza dell'ecosistema digitale di un Ateneo

Durata della prova: 2 ore

Traccia 2

PREMESSE

Contesto di riferimento

Un Ateneo pubblico di grandi dimensioni supporta le proprie attività didattiche, di ricerca e amministrativogestionali mediante un ecosistema ICT articolato ed eterogeneo.

L'attuale architettura comprende:

- due data center di Ateneo, nei quali sono ospitati server fisici, infrastrutture virtualizzate, sistemi di storage e database enterprise;

- infrastrutture cloud pubbliche e private utilizzate secondo modelli IaaS e PaaS;

- servizi SaaS, tra cui Microsoft 365, piattaforme per la collaborazione, applicazioni amministrative e servizi specialistici;

- un sistema centralizzato di Identity and Access Management, integrato con Active Directory, servizi di Single Sign-On e federazioni di identità;

- database Oracle, Microsoft SQL Server e PostgreSQL, gestiti da gruppi tecnici differenti;

- piattaforme per la didattica digitale e laboratori informatici utilizzati dagli studenti;

- infrastrutture HPC e cluster GPU a supporto della ricerca scientifica, della data science e delle applicazioni di intelligenza artificiale;

- sistemi di backup e replica differenziati, non sempre governati secondo standard omogenei;

- strumenti di monitoraggio, logging e sicurezza gestiti da più unità organizzative e fornitori esterni.

Nel corso degli anni i servizi sono stati sviluppati o acquisiti in modo progressivo, con conseguente

eterogeneità delle tecnologie, delle modalità di gestione e dei livelli di servizio.

L'Ateneo è classificato come soggetto importante ai sensi della normativa NIS2 e intende rafforzare il proprio sistema di gestione della sicurezza, perseguendo inoltre, per il perimetro della Direzione ICT, un progressivo allineamento alla norma ISO/IEC 27001.

Problematiche rilevate

Un'analisi preliminare ha evidenziato le seguenti criticità:

- assenza di una classificazione unitaria dei servizi in base a criticità, requisiti di disponibilità e sensibilità dei

dati trattati;

- dipendenze tra sistemi on premises, cloud e SaaS non completamente documentate;

- procedure di provisioning e deprovisioning delle utenze non uniformi, in particolare per collaboratori,

ospiti, ricercatori e soggetti esterni;

- presenza di account amministrativi permanenti e privilegi non sempre sottoposti a revisione periodica;

- strumenti di monitoraggio, logging e rilevazione degli incidenti non pienamente integrati;

- strategie di backup, replica e Disaster Recovery differenziate tra i diversi servizi;

- test di ripristino e continuità operativa effettuati in modo non sistematico;

- utilizzo crescente di servizi cloud e SaaS, con rischi di dipendenza tecnologica e contrattuale dai fornitori;

- crescita della domanda di risorse HPC, GPU e piattaforme per applicazioni di intelligenza artificiale;

- frammentazione delle responsabilità tra unità ICT centrali, strutture dipartimentali, responsabili applicativi e fornitori esterni.

Evento scatenante: indisponibilità di servizi cloud e crisi di portabilità dei dati e delle applicazioni

L'Ateneo utilizza da alcuni anni un'importante piattaforma cloud pubblica per l'erogazione di servizi applicativi, ambienti di sviluppo, database gestiti, sistemi di analisi dei dati e risorse di calcolo destinate alla ricerca.

A seguito di un guasto esteso presso la regione cloud utilizzata dall'Ateneo, alcuni servizi IaaS e PaaS sono risultati indisponibili per circa dodici ore. L'evento ha interessato contemporaneamente:

- applicazioni utilizzate per la didattica;

- componenti di integrazione con i sistemi amministrativi;

- database gestiti;

- ambienti di sviluppo e test;

- repository contenenti dati e modelli utilizzati per attività di machine learning;

- sistemi di autenticazione e autorizzazione integrati con servizi cloud;

- risorse GPU utilizzate da gruppi di ricerca.

Durante l'incidente è emerso che alcune applicazioni, formalmente considerate ridondate, dipendevano in realtà da servizi collocati nella medesima regione cloud o da componenti PaaS non facilmente replicabili presso un altro fornitore.

Il ripristino è stato inoltre rallentato dalla difficoltà di:

- ricostruire le configurazioni degli ambienti;

- trasferire rapidamente grandi quantità di dati;

- ripristinare i database su infrastrutture alternative;

- reperire personale con competenze adeguate sulle specifiche tecnologie proprietarie utilizzate;

- verificare la compatibilità delle applicazioni con ambienti differenti;

- coordinare le attività tra fornitori cloud, gruppi tecnici interni e responsabili dei servizi.

- Nei mesi successivi il fornitore ha inoltre comunicato:

- una significativa revisione delle condizioni economiche;

- la dismissione programmata di alcuni servizi PaaS utilizzati dall'Ateneo;

- modifiche alle modalità di esportazione dei dati;

- nuovi vincoli contrattuali relativi alla localizzazione di alcune componenti del servizio.

- L'evento ha evidenziato:

- l’assenza di criteri uniformi per la scelta tra on premises, IaaS, PaaS e SaaS;

- un’elevata dipendenza da servizi e interfacce proprietarie;

- la mancanza di un’architettura formalmente progettata per la portabilità delle applicazioni;

- l’insufficiente documentazione delle dipendenze tra componenti on premises e cloud;

- la presenza di dati e configurazioni non facilmente esportabili;

- l’assenza di strategie di uscita formalizzate per i principali fornitori;

- la difficoltà di garantire RTO e RPO in presenza di indisponibilità estese del cloud provider;

- la mancata valutazione sistematica dei rischi di concentrazione tecnologica e contrattuale;

- criticità nella gestione delle chiavi crittografiche e dei sistemi di identità in scenari di indisponibilità del fornitore;

- la necessità di bilanciare scalabilità, innovazione, sostenibilità economica e Digital Sovereignty;

- l’assenza di un modello unitario per la gestione delle risorse di calcolo destinate a data science, intelligenza artificiale e HPC.

Assegnazione progetto strategico

A seguito dell’evento, la Direzione Generale dell’Ateneo ha chiesto di predisporre un progetto organico di evoluzione dell’ecosistema ICT, da realizzare nell’arco di tre anni e finalizzato a:

- migliorare la resilienza, la sicurezza e la continuità dei servizi;

- razionalizzare l’architettura e le modalità di gestione degli ambienti on premises e in cloud;

- rafforzare il governo delle identità, dei dati, delle infrastrutture e dei fornitori;

- definire responsabilità, processi operativi e livelli di servizio coerenti con la criticità dei sistemi;

- assicurare sostenibilità tecnologica, economica e organizzativa, limitando i rischi di dipendenza da singoli fornitori o tecnologie.

Il progetto dovrà assicurare la resilienza dei servizi anche rispetto a indisponibilità prolungate dei fornitori, definendo adeguate strategie di portabilità, interoperabilità, continuità operativa e governo delle dipendenze tecnologiche e contrattuali.

Vincoli

La proposta dovrà tenere conto dei seguenti vincoli:

- necessità di garantire la continuità dei servizi durante la trasformazione;

- presenza di sistemi legacy e di contratti pluriennali non immediatamente modificabili;

- disponibilità limitata di risorse economiche e competenze specialistiche;

- distribuzione delle responsabilità tra strutture ICT centrali, dipartimenti, responsabili applicativi e fornitori;

- rispetto degli obblighi normativi applicabili, con particolare riferimento alla sicurezza informatica, alla

protezione dei dati e alla normativa NIS2;

- necessità di preservare l’autonomia della ricerca, nel rispetto di requisiti comuni di sicurezza e governance.

Il candidato potrà formulare ulteriori ipotesi, purché siano esplicitate e coerenti con il contesto.

RICHIESTA

Il candidato, assumendo il ruolo di responsabile del progetto di cui alle PREMESSE, elabori una proposta di intervento articolata nelle seguenti sezioni:

1. Analisi e priorità

Individuazione dei principali requisiti, vincoli, rischi e dipendenze emersi dal caso, con indicazione delle priorità di intervento.

2. Soluzione tecnico-organizzativa

Descrizione dell'architettura e del modello operativo proposti, evidenziando:

- le principali scelte relative a infrastrutture on premises e in cloudst;

- le misure di sicurezza, resilienza e protezione dei dati;

- le modalità di gestione delle identità, degli accessi e dei sistemi critici;

- il modello di governance e la ripartizione delle responsabilità.

La proposta dovrà approfondire gli aspetti maggiormente rilevanti rispetto all'evento di riferimento. Non è richiesta una trattazione analitica di tutte le tecnologie e di tutti i processi presenti nel contesto.

3. Piano di attuazione

Articolazione del programma in un numero limitato di fasi, distinguendo almeno:

- interventi urgenti;

- interventi di consolidamento;

- interventi strutturali.

Per ciascuna fase dovranno essere indicati i principali risultati attesi, le dipendenze e le responsabilità.

4. Verifica dei risultati

Individuazione di un insieme essenziale di indicatori utili a misurare l'efficacia degli interventi, con particolare riferimento a disponibilità, sicurezza, capacità di ripristino, qualità del servizio e avanzamento del programma.

Indicazioni per lo svolgimento

La proposta dovrà avere carattere progettuale e non meramente descrittivo.

Non è richiesto:

- il dimensionamento analitico delle infrastrutture;

- il calcolo dettagliato dei costi;

- il riferimento obbligatorio a specifici prodotti commerciali;

- lo sviluppo completo di procedure operative o documenti di conformità.

Le soluzioni proposte dovranno essere motivate in relazione ai requisiti, ai rischi e ai vincoli individuati.

PROVA PROGETTUALE

Progettazione dell'evoluzione, della sicurezza e della resilienza dell'ecosistema digitale di un Ateneo

Durata della prova: 2 ore

Traccia 3

PREMESSE

Contesto di riferimento

Un Ateneo pubblico di grandi dimensioni supporta le proprie attività didattiche, di ricerca e amministrativogestionali mediante un ecosistema ICT articolato ed eterogeneo.

L'attuale architettura comprende:

- due data center di Ateneo, nei quali sono ospitati server fisici, infrastrutture virtualizzate, sistemi di storage e database enterprise;

- infrastrutture cloud pubbliche e private utilizzate secondo modelli IaaS e PaaS;

- servizi SaaS, tra cui Microsoft 365, piattaforme per la collaborazione, applicazioni amministrative e servizi specialistici;

- un sistema centralizzato di Identity and Access Management, integrato con Active Directory, servizi di Single Sign-On e federazioni di identità;

- database Oracle, Microsoft SQL Server e PostgreSQL, gestiti da gruppi tecnici differenti;

- piattaforme per la didattica digitale e laboratori informatici utilizzati dagli studenti;

- infrastrutture HPC e cluster GPU a supporto della ricerca scientifica, della data science e delle applicazioni di intelligenza artificiale;

- sistemi di backup e replica differenziati, non sempre governati secondo standard omogenei;

- strumenti di monitoraggio, logging e sicurezza gestiti da più unità organizzative e fornitori esterni.

Nel corso degli anni i servizi sono stati sviluppati o acquisiti in modo progressivo, con conseguente eterogeneità delle tecnologie, delle modalità di gestione e dei livelli di servizio.

L'Ateneo è classificato come soggetto importante ai sensi della normativa NIS2 e intende rafforzare il proprio sistema di gestione della sicurezza, perseguendo inoltre, per il perimetro della Direzione ICT, un progressivo allineamento alla norma ISO/IEC 27001.

Problematiche rilevate

Un'analisi preliminare ha evidenziato le seguenti criticità:

- assenza di una classificazione unitaria dei servizi in base a criticità, requisiti di disponibilità e sensibilità dei dati trattati;

- dipendenze tra sistemi on premises, cloud e SaaS non completamente documentate;

- procedure di provisioning e deprovisioning delle utenze non uniformi, in particolare per collaboratori,

ospiti, ricercatori e soggetti esterni;

- presenza di account amministrativi permanenti e privilegi non sempre sottoposti a revisione periodica;

- strumenti di monitoraggio, logging e rilevazione degli incidenti non pienamente integrati;

- strategie di backup, replica e Disaster Recovery differenziate tra i diversi servizi;

- test di ripristino e continuità operativa effettuati in modo non sistematico;

- utilizzo crescente di servizi cloud e SaaS, con rischi di dipendenza tecnologica e contrattuale dai fornitori;

- crescita della domanda di risorse HPC, GPU e piattaforme per applicazioni di intelligenza artificiale;

- frammentazione delle responsabilità tra unità ICT centrali, strutture dipartimentali, responsabili applicativi e fornitori esterni.

Evento scatenante: indisponibilità dell'infrastruttura HPC e continuità delle attività di ricerca

L'Ateneo dispone di un'infrastruttura centralizzata per il calcolo scientifico costituita da cluster HPC con nodi CPU e GPU, sistemi di storage ad alte prestazioni, strumenti di schedulazione dei job e ambienti software condivisi. La piattaforma è utilizzata da numerosi gruppi di ricerca per attività di simulazione, data science, machine learning e intelligenza artificiale e, in alcuni casi, tratta dati personali, riservati o soggetti a vincoli contrattuali.

Durante un periodo caratterizzato da numerose scadenze progettuali, un guasto al sistema di storage, associato a un malfunzionamento dell'impianto di raffreddamento, ha determinato l'arresto di una parte significativa dell'infrastruttura per circa quarantotto ore.

L'evento ha comportato:

- l'interruzione di elaborazioni scientifiche di lunga durata;

- la perdita di risultati intermedi non sottoposti a checkpoint;

- l'indisponibilità temporanea di dataset condivisi;

- il mancato rispetto di alcune scadenze progettuali;

- la sospensione dell'accesso alle risorse GPU;

- il trasferimento urgente di alcuni workload verso servizi cloud, con costi non previsti;

- difficoltà nel ricostruire rapidamente ambienti software e dipendenze applicative su infrastrutture alternative.

La gestione dell'incidente ha inoltre evidenziato:

- l'assenza di RTO e RPO formalmente definiti per i principali servizi HPC;

- l'insufficiente ridondanza di storage e componenti infrastrutturali;

- la mancanza di strategie uniformi di checkpoint, replica e backup;

- la difficoltà di garantire la portabilità e la riproducibilità dei workload;

- criteri non sempre formalizzati per la priorità dei job e l'allocazione delle risorse;

- una limitata capacità di previsione della domanda di CPU, GPU e storage;

- procedure non omogenee per la classificazione, il trasferimento e la conservazione dei dati della ricerca;

- criticità nella gestione degli accessi, degli account privilegiati e della segregazione tra progetti;

- una frammentazione delle responsabilità tra struttura ICT, dipartimenti, responsabili scientifici e fornitori.

La crescita della domanda di risorse GPU ha inoltre aperto un confronto tra l'acquisizione di nuove infrastrutture interne e il ricorso a servizi cloud o a infrastrutture di supercalcolo esterne.

Assegnazione progetto strategico

A seguito dell'evento, la Direzione Generale dell'Ateneo ha chiesto di predisporre un progetto organico di evoluzione dell'ecosistema ICT, da realizzare nell'arco di tre anni e con particolare riferimento alle infrastrutture per la ricerca, la data science e l'intelligenza artificiale.

- Il programma dovrà definire un modello integrato tra risorse HPC e GPU interne, servizi cloud e infrastrutture esterne, garantendo:

- resilienza e continuità operativa;

- sicurezza e protezione dei dati;

- portabilità e riproducibilità delle elaborazioni;

- criteri trasparenti di allocazione delle risorse;

- sostenibilità economica ed energetica;

- chiara attribuzione di ruoli e responsabilità;

- integrazione con i servizi di identità, monitoraggio, backup e Disaster Recovery dell'Ateneo.

Vincoli

La proposta dovrà tenere conto dei seguenti vincoli:

- necessità di garantire la continuità dei servizi durante la trasformazione;

- presenza di sistemi legacy e di contratti pluriennali non immediatamente modificabili;

- disponibilità limitata di risorse economiche e competenze specialistiche;

- distribuzione delle responsabilità tra strutture ICT centrali, dipartimenti, responsabili applicativi e fornitori;

- rispetto degli obblighi normativi applicabili, con particolare riferimento alla sicurezza informatica, alla protezione dei dati e alla normativa NIS2;

- necessità di preservare l'autonomia della ricerca, nel rispetto di requisiti comuni di sicurezza e governance.

Il candidato potrà formulare ulteriori ipotesi, purché siano esplicitate e coerenti con il contesto.

RICHIESTA

Il candidato, assumendo il ruolo di responsabile del progetto di cui alle PREMESSE, elabori una proposta di intervento articolata nelle seguenti sezioni:

1. Analisi e priorità

Individuazione dei principali requisiti, vincoli, rischi e dipendenze emersi dal caso, con indicazione delle priorità di intervento.

2. Soluzione tecnico-organizzativa

Descrizione dell'architettura e del modello operativo proposti, evidenziando:

- le principali scelte relative a infrastrutture on premises, cloud e SaaS;

- le misure di sicurezza, resilienza e protezione dei dati;

- le modaralità di gestione delle identità, degli accessi e dei sistemi critici;

- il modello di governance e la ripartizione delle responsabilità.

La proposta dovrà approfondire gli aspetti maggiormente rilevanti rispetto all'evento di riferimento. Non è richiesta una trattazione analitica di tutte le tecnologie e di tutti i processi presenti nel contesto.

3. Piano di attuazione

Articolazione del programma in un numero limitato di fasi, distinguendo almeno:

- interventi urgenti;

- interventi di consolidamento;

- interventi strutturali.

Per ciascuna fase dovranno essere indicati i principali risultati attesi, le dipendenze e le responsabilità.

4. Verifica dei risultati

Individuazione di un insieme essenziale di indicatori utili a misurare l'efficacia degli interventi, con particolare riferimento a disponibilità, sicurezza, capacità di ripristino, qualità del servizio e avanzamento del programma.

Indicazioni per lo svolgimento

La proposta dovrà avere carattere progettuale e non meramente descrittivo.

Non è richiesto:

- il dimensionamento analitico delle infrastrutture;

- il calcolo dettagliato dei costi;

- il riferimento obbligatorio a specifici prodotti commerciali;

- lo sviluppo completo di procedure operative o documenti di conformità.

Le soluzioni proposte dovranno essere motivate in relazione ai requisiti, ai rischi e ai vincoli individuati.