Esame di Stato - Ingegnere dell'Informazione

Giorno 9

5 maggio 2026 - Settimana 2

Sicurezza, integrita' dei dati e architettura

Come trasformare una traccia generica in una risposta solida da prima prova, con basi utili anche per seconda prova, pratica e orale.

Obiettivo pratico di oggi

Alla fine di questa giornata devi saper scrivere una risposta ordinata su sicurezza e integrita' dei dati in un sistema informativo. Non devi diventare esperto di cybersecurity: devi saper impostare il ragionamento, usare termini corretti e motivare le scelte.

Formula da portare in testa

Sicurezza = riservatezza + integrita' + disponibilita'. Poi aggiungi: autenticazione, autorizzazione, crittografia, log, backup, monitoraggio, gestione incidenti, privacy.

Questo giorno e' costruito sulle tendenze emerse dalle tracce caricate: sicurezza nei sistemi informativi, privacy, cloud, dati, sistemi distribuiti, AI/IoT e responsabilita' professionale dell'ingegnere.

1. Dove siamo nel piano

Siamo al Giorno 9, seconda settimana. La prima settimana serviva a sbloccare il metodo: template, struttura, risposte semplici. Ora iniziamo a fare cose piu' serie, ma sempre spiegate da zero.

Strategia confermata

- 70% prima prova: imparare a scrivere un tema tecnico-argomentativo credibile.
- 20% basi tecniche: concetti che torneranno nella seconda prova, come database, sicurezza, cloud, ingegneria del software.
- 10% pratica/orale: piccoli agganci a requisiti, architettura, UML, dati, scelte progettuali e motivazione delle scelte.

Perche' oggi sicurezza e integrita' dei dati

Questo tema e' molto intelligente da studiare adesso per tre motivi. Primo: puo' uscire come prima prova generale, perche' riguarda responsabilita', impatto sociale, privacy e qualita' dei sistemi. Secondo: e' tecnico abbastanza da aiutarti anche nella seconda prova. Terzo: e' progettuale, quindi prepara anche la prova pratica.

Le tracce che hai caricato mostrano spesso richieste su sicurezza, dati, cloud, sistemi informativi, architetture, SIEM, IDS/IPS, backup e disaster recovery. Quindi oggi non studiamo un argomento casuale: studiamo un nucleo riutilizzabile.

Piano della sessione, se hai 1 o 2 ore

Tempo	Cosa fai	Risultato
10 min	Leggi la mappa e il glossario base.	Capisci le parole minime.
25 min	Studia il template specifico per sicurezza e dati.	Sai in che ordine scrivere.
30 min	Leggi la risposta modello, non per memorizzarla ma per vedere il montaggio.	Vedi come nasce un elaborato.
20 min	Fai il mini-esercizio guidato.	Produci uno schema tuo.
25 min	Scrivi l'esercizio finale.	Hai materiale da mandare in chat per correzione.

Se hai solo un'ora

Leggi sezioni 2, 3, 5, 8 e fai l'esercizio finale ridotto. Meglio fare poco ma scritto, piuttosto che leggere tutto senza produrre.

2. Traccia tipo di oggi

Traccia simulata

Con riferimento a un sistema informativo distribuito utilizzato da una pubblica amministrazione, da un'azienda sanitaria o da un'azienda di logistica, il candidato analizzi le problematiche relative alla sicurezza e all'integrita' dei dati. Si illustrino le principali minacce, i requisiti del sistema, l'architettura generale, le misure di protezione, le strategie di backup e continuita' operativa e il ruolo dell'ingegnere dell'informazione.

Questa traccia e' volutamente ampia. All'esame potrebbe essere formulata in modo diverso: sicurezza in un sistema informativo, protezione di infrastrutture critiche, privacy nei dati sanitari, architettura sicura per una PA, piattaforma cloud, sistema logistico, sistema con sensori IoT o AI. Il nucleo della risposta resta lo stesso.

Cosa devi capire, prima di scrivere

1. Non devi elencare strumenti a caso. Devi partire dal problema: quali dati devo proteggere e da chi?
2. Devi distinguere cosa fa il sistema dai requisiti di qualita'. La sicurezza e' un requisito non funzionale, ma influenza tutta l'architettura.
3. Devi mostrare che l'ingegnere ragiona per rischi: minaccia, vulnerabilita', impatto, contromisura.
4. Devi parlare sia di prevenzione sia di risposta: non basta evitare l'attacco, serve anche rilevarlo, limitarne gli effetti e ripristinare il servizio.
5. Devi chiudere con responsabilita' professionale, privacy, continuita' e sostenibilita' delle scelte.

La frase-ancora

In un sistema informativo moderno la sicurezza non puo' essere aggiunta alla fine, ma deve essere progettata fin dall'inizio insieme ai requisiti funzionali, all'architettura, alla gestione dei dati e ai processi operativi.

3. Glossario minimo spiegato da zero

Non saltare questa sezione. Se capisci questi termini, riesci a scrivere. Se li memorizzi senza capirli, ti blocchi appena la traccia cambia forma.

Termine	Senso semplice	Frase da esame
Riservatezza	Solo chi e' autorizzato puo' vedere i dati. Esempio: un cittadino vede solo le proprie pratiche, non quelle di altri.	Il sistema deve garantire la riservatezza delle informazioni, limitando l'accesso ai soli utenti autorizzati.
Integrita'	I dati non devono essere modificati in modo non autorizzato o accidentale. Esempio: una spedizione, un referto o una pratica non devono cambiare senza traccia.	L'integrita' dei dati deve essere tutelata tramite controlli applicativi, vincoli sul database, log e tracciamento delle modifiche.
Disponibilita'	Il servizio deve essere raggiungibile quando serve. Esempio: un sistema sanitario o pubblico non puo' restare fermo per ore senza procedure di emergenza.	La disponibilita' del servizio richiede ridondanza, backup, monitoraggio e procedure di disaster recovery.
Autenticazione	Verifica chi sei. Login, password, SPID, MFA, certificati.	L'autenticazione permette di identificare l'utente prima di concedere accesso al sistema.

Termine	Senso semplice	Frase da esame
Autorizzazione	Verifica cosa puoi fare. Dopo il login, non tutti possono fare tutto.	L'autorizzazione stabilisce le operazioni consentite in base al ruolo dell'utente.
RBAC	Role Based Access Control: permessi basati sui ruoli. Esempio: operatore, amministratore, cittadino, auditor.	Un modello RBAC consente di associare a ciascun ruolo un insieme coerente di privilegi.
Crittografia	Trasforma i dati in forma non leggibile senza chiave. Serve in trasmissione e in archiviazione.	La cifratura dei dati in transito e a riposo riduce il rischio di esposizione delle informazioni sensibili.
Firewall	Filtro tra reti. Decide quale traffico puo' passare e quale no.	Il firewall costituisce un primo livello di controllo del traffico verso i servizi esposti.
IDS/IPS	IDS rileva intrusioni; IPS puo' anche bloccarle. Non sostituisce il firewall, lo completa.	Sistemi IDS/IPS consentono di individuare comportamenti anomali e tentativi di intrusione.
Log	Registrazione degli eventi: chi ha fatto cosa, quando e da dove.	I log sono essenziali per audit, tracciabilita' e ricostruzione degli incidenti.
SIEM	Sistema che raccoglie e correla log da piu' sorgenti per individuare anomalie.	Un SIEM permette il monitoraggio continuo e la correlazione degli eventi di sicurezza.
Backup	Copia dei dati. Non e' solo salvarli: bisogna anche testarli.	Backup periodici e verificati riducono il rischio di perdita dei dati.
Disaster recovery	Piano per ripartire dopo un guasto grave o un attacco.	Il disaster recovery definisce tempi, procedure e risorse per il ripristino del servizio.
RTO e RPO	RTO: entro quanto tempo devo ripartire. RPO: quanti dati posso perdere al massimo.	RTO e RPO permettono di dimensionare correttamente le strategie di continuita' operativa.
Privacy by design	La privacy si progetta fin dall'inizio, non si aggiunge dopo.	In presenza di dati personali, il sistema deve adottare principi di minimizzazione, controllo degli accessi e protezione by design.

4. Mappa mentale: dal problema alla risposta

Quando leggi una traccia sulla sicurezza, non partire dagli strumenti. Parti dai dati. La domanda nascosta e': quali informazioni devo proteggere, quali operazioni sono critiche e cosa puo' andare storto?

> **Catena logica da ricordare**
>
> Dati -> Attori -> Operazioni -> Minacce -> Requisiti -> Architettura -> Contromisure -> Monitoraggio -> Ripristino -> Responsabilita'

Esempio mentale rapidissimo

Domanda	Risposta nel caso di una PA locale
Quali dati?	Dati anagrafici, pratiche, documenti, pagamenti, comunicazioni, log di accesso.
Chi li usa?	Cittadini, operatori, responsabili, amministratori di sistema, eventuali fornitori esterni.
Cosa puo' andare storto?	Accessi abusivi, modifica non autorizzata, ransomware, indisponibilita', errore umano, fuga di dati.
Cosa serve?	Ruoli, autenticazione forte, cifratura, log, backup, firewall, monitoraggio, policy, formazione.
Come lo organizzo?	Frontend web, backend applicativo, database, servizi di identita', rete segmentata, SIEM, backup separato.

Il trucco che evita il blocco

Se non sai da dove iniziare, scrivi subito tre righe: il sistema tratta dati importanti, quindi deve proteggere riservatezza, integrita' e disponibilita'. Poi scegli un esempio concreto: PA, sanita', logistica, scuola, azienda. Da quel momento la risposta diventa gestibile.

5. Template specifico per una traccia su sicurezza e dati

Questo e' il template base adattato alla traccia di oggi. Non devi usare sempre tutti i titoli, ma devi mantenere l'ordine mentale.

Blocco	Cosa scrivere
1. Introduzione	Inquadra sicurezza e integrita' come requisiti essenziali nei sistemi informativi moderni.
2. Contesto	Scegli un esempio: PA locale, sanita', logistica, piattaforma cloud, sistema IoT.
3. Dati e attori	Specifica quali dati sono trattati e chi accede al sistema.
4. Minacce e rischi	Elenca accessi abusivi, perdita dati, manomissione, malware, DDoS, errori umani, insider.
5. Requisiti	Funzionali: gestione dati, utenti, notifiche, report. Non funzionali: sicurezza, privacy, disponibilita', scalabilita'.
6. Architettura	Frontend, backend, database, API, cloud, rete segmentata, servizi di identita', logging.
7. Contromisure	Autenticazione, autorizzazione, cifratura, firewall, IDS/IPS, backup, log, patching, formazione.
8. Continuita'	Ridondanza, backup testati, disaster recovery, RTO/RPO, monitoraggio.
9. Normativa ed etica	GDPR, minimizzazione, tracciabilita', responsabilita', proporzionalita' delle scelte.
10. Ruolo dell'ingegnere	Motiva le scelte e collega tecnologia, rischi, costi, qualita' e bisogni reali.

Blocco	Cosa scrivere
11. Conclusione	Chiudi ribadendo che la sicurezza e' parte integrante della progettazione.

Versione ultra-breve del template

Introduzione - esempio concreto - dati/attori - minacce - requisiti - architettura - misure di sicurezza - backup/continuita' - privacy/GDPR - ruolo dell'ingegnere - conclusione

6. Risposta modello completa da esame

Leggila come esempio di montaggio. Non devi copiarla a memoria. Devi capire come i pezzi si collegano.

> **Traccia modello**
>
> Il candidato illustri le principali problematiche di sicurezza e integrita' dei dati nella progettazione di un sistema informativo distribuito per una pubblica amministrazione locale, indicando requisiti, architettura, misure di protezione e responsabilita' dell'ingegnere.

Risposta modello

La gestione sicura dei dati rappresenta un aspetto centrale nella progettazione dei sistemi informativi moderni, soprattutto quando tali sistemi sono utilizzati da pubbliche amministrazioni, strutture sanitarie o aziende che trattano informazioni personali, documenti, pagamenti e servizi digitali. In questi contesti, la sicurezza non deve essere considerata come un elemento accessorio, ma come un requisito progettuale fondamentale, strettamente collegato alla qualita', all'affidabilita' e alla continuita' del servizio.

Si consideri, ad esempio, un sistema informativo per una pubblica amministrazione locale che consenta ai cittadini di consultare pratiche, caricare documenti, ricevere comunicazioni, effettuare richieste e monitorare lo stato dei procedimenti. Il sistema e' utilizzato da diversi attori: cittadini, operatori amministrativi, responsabili degli uffici, amministratori di sistema ed eventualmente fornitori esterni di servizi cloud o manutenzione. I dati trattati possono includere informazioni anagrafiche, documenti personali, stati delle pratiche, pagamenti, comunicazioni ufficiali e log delle operazioni effettuate.

In un sistema di questo tipo le principali minacce riguardano l'accesso non autorizzato ai dati, la modifica indebita delle informazioni, la perdita o indisponibilita' del servizio, l'intercettazione delle comunicazioni, gli attacchi malware o ransomware, gli errori umani e l'abuso di privilegi da parte di utenti interni. Tali minacce possono produrre effetti rilevanti: violazione della privacy, blocco dei servizi pubblici, danni economici, perdita di fiducia da parte degli utenti e responsabilita' legali per l'ente.

I requisiti funzionali del sistema riguardano le operazioni che esso deve svolgere: registrare e autenticare gli utenti, permettere la gestione delle pratiche, consentire il caricamento e la consultazione dei documenti, inviare notifiche, produrre report e gestire i diversi profili di accesso. Accanto a questi requisiti, assumono particolare importanza i requisiti non funzionali: sicurezza, privacy, disponibilita', affidabilita', usabilita', scalabilita' e manutenibilita'. Questi requisiti definiscono la qualita' complessiva del sistema e condizionano le scelte architetturali.

L'architettura puo' essere organizzata su piu' livelli. Un frontend web o mobile consente l'interazione con cittadini e operatori; un backend applicativo gestisce la logica del sistema, le regole di autorizzazione, i workflow e l'accesso ai dati; un database relazionale memorizza in modo strutturato utenti, pratiche, documenti, ruoli e log. A questi componenti si possono aggiungere servizi esterni, API, sistemi di autenticazione federata, storage documentale, moduli di monitoraggio e sistemi di backup. In caso di adozione del cloud, e' necessario distinguere chiaramente le responsabilita' del fornitore e quelle dell'ente gestore del servizio.

Dal punto di vista della sicurezza, una prima misura riguarda l'autenticazione degli utenti, eventualmente con autenticazione forte o multifattore per gli operatori e gli amministratori. L'autenticazione consente di verificare l'identita' dell'utente, mentre l'autorizzazione stabilisce quali operazioni siano consentite. Un modello basato sui ruoli, ad esempio RBAC, permette di distinguere cittadini, operatori, responsabili e amministratori, evitando che un utente possa accedere a

funzionalita' o dati non coerenti con il proprio ruolo.

La protezione delle comunicazioni deve essere garantita tramite protocolli sicuri, come HTTPS/TLS, in modo da ridurre il rischio di intercettazione dei dati in transito. I dati piu' sensibili devono inoltre essere cifrati anche a riposo, cioe' quando sono memorizzati su database o sistemi di storage. L'integrita' dei dati puo' essere rafforzata mediante vincoli sul database, transazioni, controlli applicativi, versionamento dei documenti, firme digitali o impronte crittografiche nei casi in cui sia necessario garantire la non alterazione dei contenuti.

Un ulteriore livello di protezione riguarda l'infrastruttura di rete. La separazione tra aree pubbliche e aree interne, mediante firewall, segmentazione di rete e zona DMZ, consente di limitare l'esposizione dei componenti piu' critici. Sistemi IDS e IPS possono rilevare o bloccare tentativi di intrusione, mentre strumenti di Web Application Firewall possono ridurre il rischio di attacchi rivolti alle applicazioni web. Le componenti devono inoltre essere mantenute aggiornate attraverso patch management e procedure di hardening.

La tracciabilita' e' essenziale. Ogni accesso rilevante e ogni operazione critica devono essere registrati in log consultabili e protetti da alterazioni. I log permettono di ricostruire gli eventi, individuare comportamenti anomali, supportare audit interni e gestire eventuali incidenti. In sistemi piu' complessi, un SIEM consente di raccogliere e correlare eventi provenienti da applicazioni, server, firewall e database, migliorando la capacita' di rilevare anomalie in modo tempestivo.

La disponibilita' del servizio richiede strategie di continuita' operativa. Backup periodici e verificati riducono il rischio di perdita dei dati, ma non sono sufficienti se non sono accompagnati da procedure di ripristino testate. Occorre definire RTO e RPO: il primo indica il tempo massimo accettabile per ripristinare il servizio, il secondo la quantita' massima di dati che si puo' perdere. In base a tali valori si possono progettare ridondanza, replica, sistemi di disaster recovery e monitoraggio continuo dell'infrastruttura.

In presenza di dati personali, la progettazione deve rispettare i principi di protezione dei dati personali. Il sistema deve trattare solo i dati necessari, limitare l'accesso in base al principio del minimo privilegio, prevedere tempi di conservazione coerenti, garantire trasparenza verso gli utenti e adottare misure tecniche e organizzative adeguate. Nei contesti piu' critici puo' essere necessaria anche una valutazione preventiva dei rischi sul trattamento dei dati.

Il ruolo dell'ingegnere dell'informazione e' quindi quello di tradurre un bisogno operativo in una soluzione tecnica sicura, affidabile e sostenibile. L'ingegnere deve valutare i rischi, motivare le scelte architetturali, bilanciare costi e benefici, garantire la conformita' normativa e progettare sistemi che possano evolvere nel tempo. Non basta adottare singoli strumenti di sicurezza: e' necessario costruire una strategia coerente che integri tecnologia, processi, persone e responsabilita'.

In conclusione, la sicurezza e l'integrita' dei dati sono elementi strutturali della progettazione di un sistema informativo. Una soluzione efficace deve integrare requisiti funzionali, architettura, controllo degli accessi, cifratura, monitoraggio, backup e gestione degli incidenti. Solo in questo modo il sistema puo' offrire servizi digitali affidabili, tutelare gli utenti e sostenere nel tempo l'attivita' dell'organizzazione che lo utilizza.

7. Versione breve da memorizzare

Questa e' la versione da tenere in testa. Serve quando devi ricostruire la risposta senza ricordare tutto.

Schema in 12 righe

- Un sistema informativo deve proteggere riservatezza, integrita' e disponibilita' dei dati.
- Scelgo un esempio concreto: PA locale, sanita', logistica o piattaforma cloud.
- Individuo attori e dati: utenti, operatori, amministratori, documenti, pratiche, log.
- Analizzo i rischi: accessi abusivi, manomissione, perdita dati, ransomware, indisponibilita'.
- Definisco requisiti funzionali e non funzionali.
- Propongo architettura: frontend, backend, database, API, cloud, rete segmentata.
- Gestisco identita' e permessi con autenticazione, autorizzazione e RBAC.
- Proteggo dati e comunicazioni con cifratura, HTTPS/TLS e controlli applicativi.
- Rilevo anomalie con log, audit, IDS/IPS e SIEM.
- Garantisco continuita' con backup, replica, disaster recovery, RTO e RPO.
- Considero privacy, GDPR, minimizzazione e principio del minimo privilegio.
- Concludo collegando sicurezza, qualita', responsabilita' professionale e utilita' del servizio.

Mnemonico da usare

CIA + AALB + GDPR

Sigla	Cosa significa	Perche' serve
CIA	Confidentiality, Integrity, Availability: riservatezza, integrita', disponibilita'.	E' il cuore della sicurezza.
AALB	Autenticazione, Autorizzazione, Log, Backup.	Sono le quattro misure che devi citare quasi sempre.
GDPR	Privacy, minimizzazione, protezione dei dati, responsabilita'.	Serve quando ci sono dati personali o sensibili.

8. Frasi pronte da usare all'esame

1. La sicurezza non deve essere considerata un'aggiunta successiva, ma un requisito progettuale da integrare fin dalle prime fasi di analisi.
2. La progettazione deve tutelare riservatezza, integrita' e disponibilita' dei dati trattati dal sistema.
3. L'autenticazione consente di identificare l'utente, mentre l'autorizzazione definisce le operazioni consentite in base al ruolo assegnato.
4. Un modello basato sui ruoli permette di applicare il principio del minimo privilegio e ridurre il rischio di accessi non autorizzati.
5. La cifratura dei dati in transito e a riposo riduce il rischio di esposizione delle informazioni in caso di intercettazione o compromissione dei sistemi.
6. I log e le procedure di audit consentono di garantire tracciabilita', individuare anomalie e ricostruire gli eventi in caso di incidente.
7. Firewall, IDS e IPS non sostituiscono una corretta progettazione applicativa, ma costituiscono livelli complementari di difesa.
8. La continuita' operativa richiede backup verificati, procedure di ripristino, monitoraggio e definizione di RTO e RPO.
9. In presenza di dati personali, il sistema deve rispettare i principi di minimizzazione, limitazione degli accessi e protezione by design.
10. Il ruolo dell'ingegnere e' motivare le scelte tecniche in relazione ai rischi, ai vincoli economici, alla normativa e agli obiettivi dell'organizzazione.
11. La sicurezza efficace nasce dalla combinazione di tecnologia, processi, formazione degli utenti e responsabilita' organizzative.
12. Una soluzione scalabile e manutenibile deve poter evolvere nel tempo senza compromettere la protezione dei dati e la continuita' del servizio.

> **Come usarle senza sembrare meccanico**
>
> Non inserire tutte le frasi. Scegline 5-6 e adattale al contesto della traccia. Una frase buona vale piu' di dieci strumenti elencati senza logica.

9. Errori da evitare

Errore	Perche' e' debole	Come correggerlo
Elencare strumenti a caso	Sembra memoria, non progetto.	Parti da dati, minacce e requisiti; poi scegli gli strumenti.
Dire solo firewall e password	E' troppo povero per Sezione A.	Aggiungi RBAC, cifratura, log, backup, monitoraggio, incident response.
Confondere autenticazione e autorizzazione	Errore tecnico frequente.	Autenticazione = chi sei; autorizzazione = cosa puoi fare.
Dimenticare integrita'	Molti parlano solo di privacy.	Cita vincoli DB, transazioni, log, versionamento, firme/hash.
Dimenticare continuita' operativa	La sicurezza non e' solo prevenzione.	Parla di backup, RTO, RPO, disaster recovery.
Parlare di GDPR in modo generico	Rischia di sembrare frase vuota.	Collega GDPR a minimizzazione, ruoli, retention, tracciabilita'.

10. Aggancio leggero alla seconda prova

Non facciamo ora una simulazione completa della seconda prova. Pero' fissiamo i concetti tecnici che possono tornare. Questa sezione serve a costruire base senza rubare la giornata alla prima prova.

Database: cosa devi sapere davvero

> **Idea semplice**
>
> Un database relazionale organizza i dati in tabelle collegate tra loro. E' adatto quando le relazioni sono importanti: utenti-ruoli, pratiche-documenti, spedizioni-veicoli, pazienti-referti.

Concetto	Spiegazione
Chiave primaria	Identifica un record in modo univoco. Esempio: id_utente.
Chiave esterna	Collega una tabella a un'altra. Esempio: id_ruolo in Utente punta a Ruolo.
Vincoli	Impediscono dati incoerenti. Esempio: una pratica deve appartenere a un utente esistente.
Transazione	Insieme di operazioni che devono riuscire tutte o fallire tutte.
ACID	Atomicita', consistenza, isolamento, durabilita': proprieta' delle transazioni.
Indice	Struttura che velocizza le ricerche, ma va usata con criterio.

Sicurezza software: micro-schema

```
Input utente -> validazione -> logica applicativa -> controllo permessi -> database
                     |                   |                        |
                sanitizzazione      audit/log               transazione
```

Senso: prima di salvare o leggere dati, il backend deve controllare che l'input sia valido, che l'utente sia autorizzato e che l'operazione venga tracciata.

Cloud: frase sufficiente per ora

L'adozione del cloud puo' migliorare scalabilita', disponibilita' e gestione delle risorse, ma richiede una chiara definizione delle responsabilita', adeguate misure di sicurezza, controllo degli accessi, cifratura, monitoraggio e piani di continuita'.

11. Aggancio alla prova pratica: architettura testuale

Questa parte non e' una simulazione pratica completa. E' un micro-aggancio: devi iniziare a vedere come una risposta argomentativa puo' diventare schema progettuale.

Schema architetturale minimo per un sistema sicuro

```
Utenti Internet
     |
     v
[DNS / HTTPS]
     |
     v
[Firewall / WAF]
     |
     v
[Reverse Proxy / DMZ]
     |
```

```
     v
[Backend applicativo / API] ----> [Identity Provider: login, MFA, ruoli]
     |
     |----> [Database relazionale cifrato]
     |----> [Storage documentale cifrato]
     |----> [Sistema di log e SIEM]
     |----> [Backup separato + Disaster Recovery]
```

Componenti e funzioni

Componente	Funzione	Perche' lo cito all'esame
Frontend	Interfaccia web/mobile per utenti e operatori.	Mostra il livello di interazione.
Backend	Gestisce regole, workflow, controlli, permessi.	E' il motore del sistema.
Database	Memorizza dati strutturati e relazioni.	Serve per integrita' e interrogazioni.
Identity provider	Gestisce autenticazione, MFA, sessioni e ruoli.	Collega sicurezza e ruoli.
Firewall/WAF	Filtra traffico e protegge applicazioni web.	Mostra difesa perimetrale.
IDS/IPS	Rileva o blocca intrusioni.	Mostra monitoraggio attivo.
SIEM	Raccoglie e correla eventi.	Mostra tracciabilita' e rilevamento anomalie.
Backup/DR	Permette ripristino in caso di guasto o attacco.	Mostra continuita' operativa.

12. Micro-modello dati utile per la pratica

Non devi ancora progettare tutto. Ma devi iniziare a ragionare per entita'. Questo e' un esempio riutilizzabile in molte tracce.

Entita' principali

Entita'	Attributi possibili	Relazioni
Utente	id_utente, nome, email, password_hash, stato	Ha uno o piu' ruoli; effettua operazioni.
Ruolo	id_ruolo, nome_ruolo	Esempi: cittadino, operatore, admin, auditor.
Permesso	id_permesso, azione, risorsa	Collegato ai ruoli.
Pratica/Documento	id, tipo, stato, data, proprietario	Appartiene a un utente o a un procedimento.
LogEvento	id_log, utente, azione, timestamp, esito, ip	Registra le operazioni rilevanti.
Backup	id_backup, data, esito, tipo, posizione	Serve per controllo e ripristino.

Schema logico minimo, solo per capire

```
UTENTE(id_utente PK, nome, email, password_hash, stato)
RUOLO(id_ruolo PK, nome)
UTENTE_RUOLO(id_utente FK, id_ruolo FK)
PERMESSO(id_permesso PK, azione, risorsa)
RUOLO_PERMESSO(id_ruolo FK, id_permesso FK)
DOCUMENTO(id_documento PK, proprietario FK, tipo, stato, data_creazione)
LOG_EVENTO(id_log PK, id_utente FK, azione, risorsa, timestamp, esito, ip)
BACKUP(id_backup PK, data_esecuzione, tipo, esito, posizione)
```

Tre query SQL da riconoscere

```
-- 1. Operazioni effettuate da un utente
SELECT azione, risorsa, timestamp, esito
FROM LOG_EVENTO
WHERE id_utente = 10
ORDER BY timestamp DESC;

-- 2. Tentativi di accesso falliti nell'ultimo giorno
SELECT id_utente, COUNT(*) AS tentativi_falliti
FROM LOG_EVENTO
WHERE azione = 'LOGIN' AND esito = 'FALLITO'
  AND timestamp >= CURRENT_DATE - INTERVAL '1 day'
GROUP BY id_utente;

-- 3. Documenti visibili da un utente proprietario
SELECT id_documento, tipo, stato, data_creazione
FROM DOCUMENTO
WHERE proprietario = 10;
```

Non devi imparare SQL oggi

Devi solo capire che la prova pratica puo' chiedere di passare da requisiti e attori a dati, tabelle e interrogazioni. Oggi il collegamento lo vedi, non lo devi padroneggiare.

13. Aggancio all'orale: domande probabili

Domanda	Risposta breve
Qual e' la differenza tra autenticazione e autorizzazione?	L'autenticazione identifica l'utente; l'autorizzazione stabilisce quali operazioni puo' svolgere.

Domanda	Risposta breve
Perche' non basta il firewall?	Perche' la sicurezza richiede piu' livelli: applicazione, dati, utenti, rete, log, monitoraggio e ripristino.
Perche' i log sono importanti?	Permettono tracciabilita', audit e ricostruzione degli eventi in caso di incidente.
Cosa sono RTO e RPO?	RTO e' il tempo massimo di ripristino; RPO e' la perdita massima di dati accettabile.
Cosa significa privacy by design?	Progettare la protezione dei dati fin dall'inizio, non come aggiunta successiva.
Qual e' il ruolo dell'ingegnere?	Valutare rischi, motivare scelte, garantire sicurezza, affidabilita', conformita' e sostenibilita'.

14. Come adattare questa risposta a tracce diverse

Una traccia puo' cambiare forma, ma puoi ricondurla allo stesso nucleo. Qui sotto trovi gli adattamenti piu' utili.

Se la traccia parla di...	Adattamento
Sanita' digitale	Enfatizza dati sensibili, referti, pazienti, accessi per ruoli, audit, GDPR, disponibilita' del servizio.
Infrastrutture critiche	Enfatizza continuita', segmentazione, IDS/IPS, risposta agli incidenti, resilienza e impatto sociale.
AI o machine learning	Aggiungi qualita' del dataset, bias, spiegabilita', controllo umano, sicurezza dei dati di addestramento.
Cloud	Aggiungi scalabilita', shared responsibility, cifratura, backup geografico, monitoraggio e controllo accessi.
Logistica	Parla di tracciamento spedizioni, veicoli, documenti, clienti, disponibilita' real-time e integrita' dello stato spedizione.
Proposta di progetto	Trasforma il tema in obiettivi, requisiti, architettura, costi, rischi, cronoprogramma e benefici.
Sistemi IoT	Aggiungi sensori, raccolta dati, autenticazione dispositivi, rete, edge/cloud, anomalie, aggiornamenti firmware.

Esempio: versione sanita' digitale in 8 righe

In un sistema sanitario digitale la sicurezza assume particolare rilevanza poiche' vengono trattati dati personali e sanitari. Il sistema deve prevedere autenticazione forte, autorizzazione basata sui ruoli, cifratura dei dati e tracciamento degli accessi. Medici, pazienti, amministrativi e tecnici devono disporre di permessi differenti. L'integrita' dei referti e delle cartelle cliniche deve essere garantita tramite controlli applicativi, versionamento e audit log. La disponibilita' e' essenziale per la continuita' assistenziale, quindi sono necessari backup, replica e disaster recovery. L'ingegnere deve progettare il sistema secondo criteri di privacy by design, minimizzazione e sicurezza operativa.

Esempio: versione logistica in 8 righe

In un sistema informativo logistico la sicurezza e l'integrita' dei dati sono fondamentali per garantire il corretto monitoraggio delle spedizioni, l'assegnazione dei veicoli e la gestione dei documenti contrattuali. Alterazioni non autorizzate dello stato di una spedizione o indisponibilita' del sistema possono generare danni economici e disservizi. Il sistema deve quindi prevedere ruoli distinti, autenticazione, autorizzazione, log delle operazioni, cifratura delle comunicazioni e backup. La tracciabilita' degli eventi consente di ricostruire responsabilita' e anomalie. L'architettura dovra' integrare frontend, backend, database, monitoraggio e procedure di ripristino.

15. Mini-esercizio guidato

Fallo con calma. Non devi scrivere un tema completo: devi riempire lo scheletro. Tempo consigliato: 15 minuti.

Traccia dell'esercizio

Sistema di prenotazione sanitaria online per visite, referti e comunicazioni tra pazienti, medici e segreteria. Analizza sicurezza e integrita' dei dati.

Completa la tabella

Blocco	Da completare
Attori	Esempio: paziente, medico, segreteria, amministratore. Aggiungi tu: ...
Dati	Esempio: prenotazioni, referti, anagrafica, log accessi. Aggiungi tu: ...
Rischi	Esempio: accesso abusivo ai referti, modifica prenotazioni, perdita dati. Aggiungi tu: ...
Requisiti non funzionali	Esempio: sicurezza, privacy, disponibilita', usabilita'. Aggiungi tu: ...
Misure	Esempio: login forte, ruoli, cifratura, log, backup. Aggiungi tu: ...
Conclusione	Scrivi una frase: Il sistema e' valido perche' ...

Poi scrivi 6 righe usando questo avvio

> Il sistema di prenotazione sanitaria online tratta dati personali e sanitari, quindi deve essere progettato con particolare attenzione a sicurezza, privacy e integrita' delle informazioni. Gli attori principali sono...

16. Esercizio finale da mandare in chat

Tempo consigliato: 20-25 minuti. Non cercare perfezione. Io poi lo correggo.

> **Traccia finale**
>
> Scegli un sistema tra: sanita' digitale, pubblica amministrazione, logistica, piattaforma scolastica. Scrivi una risposta di 18-25 righe sul tema: sicurezza e integrita' dei dati. Devi includere: dati, attori, rischi, architettura, misure di sicurezza, backup/continuita', privacy e ruolo dell'ingegnere.

Schema da seguire

1. Introduzione: perche' il tema e' importante.
2. Esempio scelto e attori.
3. Dati trattati.
4. Rischi principali.
5. Architettura generale.
6. Misure: autenticazione, autorizzazione, cifratura, log, firewall/IDS/IPS.
7. Backup, disaster recovery, disponibilita'.
8. Privacy/GDPR se ci sono dati personali.
9. Ruolo dell'ingegnere e conclusione.

> **Regola**
>
> Non scrivere solo elenco. Ogni 3-4 righe collega: problema -> scelta tecnica -> motivo. Esempio: 'Poiche' i referti sono dati sensibili, e' necessario limitare gli accessi tramite ruoli e registrare le operazioni in log'.

17. Checklist di autocorrezione

Controllo	Ok
Ho scritto un'introduzione chiara?	
Ho scelto un esempio concreto?	
Ho indicato dati e attori?	
Ho distinto requisiti funzionali e non funzionali?	
Ho citato almeno 4 rischi?	
Ho citato autenticazione e autorizzazione senza confonderle?	
Ho parlato di cifratura, log e backup?	
Ho incluso disponibilita' e disaster recovery?	
Ho collegato privacy/GDPR al caso concreto?	
Ho concluso con il ruolo dell'ingegnere?	

Livelli indicativi

Livello	Com'e' la risposta
Insufficiente	Elenco confuso, niente esempio, strumenti citati a caso, poca sicurezza reale.
Base	Esempio presente, alcuni requisiti e misure, ma poca architettura o poca motivazione.
Buono	Struttura chiara, dati/attori/rischi, architettura, misure e privacy ben collegate.
Molto buono	Risposta completa, tecnica ma comprensibile, con ruolo dell'ingegnere, continuita' operativa e responsabilita'.

18. Schede memoria: ripasso in 5 minuti

Ripeti queste schede a voce. Sono costruite per fissare, non per studiare altra teoria.

Domanda	Risposta
Quali sono i tre pilastri della sicurezza?	Riservatezza, integrita', disponibilita'.
Differenza tra autenticazione e autorizzazione?	Autenticazione: chi sei. Autorizzazione: cosa puoi fare.
A cosa servono i log?	A tracciare operazioni, fare audit, rilevare anomalie e ricostruire incidenti.
Perche' servono i backup?	Per ridurre il rischio di perdita dati e ripristinare il servizio dopo guasti o attacchi.
Cosa significa privacy by design?	Progettare la tutela dei dati fin dall'inizio.
Cos'e' un IDS/IPS?	IDS rileva intrusioni; IPS puo' bloccarle.
Cos'e' RTO?	Tempo massimo accettabile per ripristinare il servizio.
Cos'e' RPO?	Quantita' massima di dati che si puo' perdere.
Frase jolly	La sicurezza deve essere integrata nei requisiti, nell'architettura e nei processi operativi.

Se all'esame vai in bianco

Procedura di emergenza

- Scrivi: 'Il sistema tratta dati rilevanti e deve tutelare riservatezza, integrita' e disponibilita'.'
- Scegli un esempio concreto.
- Elenca attori e dati.
- Scrivi 4 rischi.
- Scrivi architettura a tre livelli: frontend, backend, database.
- Aggiungi: ruoli, cifratura, log, backup, monitoraggio.
- Chiudi con privacy e ruolo dell'ingegnere.

19. Perche' questo giorno e' strategico

Questa giornata e' stata costruita per essere utile su piu' fronti: prima prova, seconda prova, pratica e orale. Il tema sicurezza-dati-architettura ricorre in forme diverse nelle tracce reali caricate: sicurezza nei sistemi informativi, architettura sicura per pubbliche amministrazioni, sistemi distribuiti, cloud, AI, dati, IoT, sanita' digitale, logistica e responsabilita' professionale.

La scelta di oggi non significa trascurare gli altri argomenti. Significa costruire un nucleo forte che puoi riutilizzare in molte tracce. Se impari bene questo, avrai gia' un linguaggio credibile per parlare di sistemi informativi, privacy, affidabilita', cloud, cyber security e progettazione.

Cosa mandare in chat per la correzione

Mandami l'esercizio finale scritto da te. Anche se e' incompleto. Correggero': struttura, contenuto, termini tecnici, frasi deboli, ordine logico e livello indicativo.

Compito minimo se sei in ritardo

Scrivi solo 12 righe su un sistema sanitario o logistico. Devono contenere almeno queste parole: dati, attori, rischio, autenticazione, autorizzazione, cifratura, log, backup, privacy, ingegnere.

Fine Giorno 9

Oggi non hai studiato 'cybersecurity' in astratto. Hai imparato a montare una risposta da esame su sicurezza, integrita' dei dati e architettura. Questo e' esattamente il tipo di competenza che serve quando la traccia e' ampia e devi dimostrare metodo.