Giorno 3 - Mercoledì 29 aprile 2026

Prima prova scritta - Cybersecurity e sicurezza dei sistemi informativi

Obiettivo della giornata

Imparare a scrivere una risposta ordinata su sicurezza informatica, senza partire da teoria astratta. Oggi devi capire il lessico minimo, riconoscere le parti della traccia e costruire una mini-risposta correggibile.

Regola personale

Non devi ricordare tutto. Devi imparare a ragionare così: che cosa devo proteggere? da chi o da cosa? con quali misure? cosa succede se qualcosa va storto?

Tempo consigliato: 1-2 ore. Priorità: prima prova. Le parti utili a seconda prova, prova pratica e orale sono segnalate solo in modo leggero.

1. Dove siamo nel piano

Nel Giorno 1 hai imparato il template base per una traccia di progettazione: scopo, attori, requisiti, architettura, dati, sicurezza e conclusione. Nel Giorno 2 hai iniziato a usare una traccia tecnologica su AI e Machine Learning. Oggi facciamo un passo molto importante: la cybersecurity.

La cybersecurity è un tema molto adatto alla prima prova perché può comparire sia come argomento principale sia come sezione dentro qualsiasi altra traccia: sistema informativo, sanità digitale, PA, azienda, cloud, IoT, AI.

> **Perché è un tema strategico**
> Se impari a parlare bene di sicurezza, puoi usarla in quasi tutte le risposte. Anche quando la traccia non dice esplicitamente 'cybersecurity', puoi aggiungere una sezione su accessi, protezione dati, backup, log e continuità operativa.

Obiettivo pratico di oggi

```
Entro fine sessione devi produrre una mini-risposta da 10-12 righe su:

Sicurezza informatica di un sistema informativo di una Pubblica Amministrazione o di un'infrastruttura critica.

Non deve essere perfetta. Deve essere strutturata.
```

2. Perché questo argomento è realistico

Dalle prove che abbiamo analizzato, la sicurezza compare in modo diretto o indiretto. Per esempio, una prova Campus 2024 chiedeva le problematiche di sicurezza informatica nella gestione delle infrastrutture critiche, citando minacce, firewall, intrusion detection, crittografia, risposta agli incidenti e implicazioni normative. Nel 2025 compaiono anche sicurezza, qualità, digitalizzazione, IoT, Big Data e AI.

Quindi questo argomento non è scelto a caso. È un nucleo trasversale: ti serve per Campus se restasse opzione, ma anche per Sapienza, Tor Vergata o Roma Tre, perché è pienamente coerente con Ingegneria dell'Informazione.

Cosa NON fare oggi

- Non studiare reti in modo dettagliato: protocolli, subnetting e routing li faremo più avanti.
- Non imparare a memoria liste infinite di attacchi.
- Non trasformare la risposta in un catalogo di strumenti senza spiegare perché servono.
- Non usare parole come firewall, IDS o crittografia se non sai dire in una frase semplice cosa fanno.

Cosa fare invece

- Capire il problema: un sistema informatico ha dati, utenti e servizi da proteggere.
- Individuare minacce e rischi.
- Proporre contromisure semplici e sensate.
- Concludere parlando di responsabilità dell'ingegnere e continuità del servizio.

3. Prima idea da fissare

Cybersecurity in una frase

La cybersecurity è l'insieme di misure tecniche, organizzative e procedurali usate per proteggere sistemi, dati e servizi da accessi non autorizzati, errori, guasti e attacchi.

Non è solo installare un antivirus. È un modo di progettare e gestire un sistema chiedendosi sempre: chi può accedere? quali dati sono sensibili? cosa succede se un servizio si blocca? come scopro un problema? come recupero?

I tre obiettivi fondamentali: RID

Per ricordare la sicurezza puoi usare la sigla RID:

Lettera	Obiettivo	Significato semplice	Esempio
R	Riservatezza	Solo chi è autorizzato può vedere i dati.	Un cittadino vede solo le proprie pratiche, non quelle di altri.
I	Integrità	I dati non devono essere modificati in modo scorretto o non autorizzato.	Un pagamento o un voto non devono essere alterati.
D	Disponibilità	Il servizio deve funzionare quando serve.	Il portale della PA deve essere raggiungibile anche in periodi critici.

Sistema di memoria

Quando parli di sicurezza, torna sempre a RID: riservatezza, integrità, disponibilità. Se citi questi tre obiettivi e li colleghi a esempi concreti, la risposta sembra subito più solida.

4. Parole base spiegate da zero

Questa pagina serve a non bloccarti davanti ai termini. Non devi recitare definizioni perfette: devi saperli usare in una frase d'esame.

Termine	Significato semplice	Frase da esame
Asset	Qualcosa da proteggere: dati, server, applicazioni, account, servizi.	Il primo passo consiste nell'individuare gli asset critici, come database, applicazioni e credenziali.
Minaccia	Evento o soggetto che può causare un danno.	Tra le minacce rientrano phishing, malware, accessi abusivi e attacchi DDoS.
Vulnerabilità	Punto debole del sistema.	Una password debole o un software non aggiornato rappresentano vulnerabilità sfruttabili.
Rischio	Possibilità che una minaccia sfrutti una vulnerabilità causando un danno.	Il rischio va valutato considerando probabilità e impatto.
Contromisura	Misura che riduce il rischio.	Firewall, autenticazione forte, backup e logging sono esempi di contromisure.
Incidente	Evento di sicurezza realmente accaduto.	In caso di incidente è necessario attivare procedure di risposta e ripristino.

Formula da ricordare

Rischio = asset importante + vulnerabilità + minaccia + possibile impatto.

Esempio: database dei cittadini + password debole + attacco phishing = furto di dati personali.

5. Strumenti di sicurezza: cosa sono e come spiegarli

Queste parole compaiono spesso nelle tracce. Per ora ti basta capirne il senso, non i dettagli tecnici.

Strumento	Cosa fa	Come usarlo nella risposta
Autenticazione	Verifica chi sei.	L'accesso deve avvenire tramite credenziali personali e, per ruoli critici, autenticazione a più fattori.
Autorizzazione	Stabilisce cosa puoi fare.	Ogni utente deve avere permessi coerenti con il proprio ruolo.
MFA	Richiede più di una prova di identità.	La MFA riduce il rischio di accesso abusivo anche in caso di password compromessa.
Cifratura	Rende i dati illeggibili senza chiave.	Le comunicazioni devono essere cifrate tramite HTTPS e i dati sensibili protetti anche a riposo.
Hashing password	Memorizza una impronta della password, non la password in chiaro.	Le password non devono essere salvate in chiaro, ma tramite hashing sicuro.
Firewall	Filtra il traffico consentito o bloccato.	Il firewall limita le comunicazioni verso i soli servizi necessari.
IDS/IPS	Rileva o blocca comportamenti sospetti.	Un sistema di rilevamento intrusioni aiuta a individuare attacchi o anomalie.
Backup	Copia dei dati per ripristinare il servizio.	Backup periodici e testati riducono il rischio di perdita dati.
Log	Registro delle operazioni.	I log consentono tracciabilità, audit e analisi degli incidenti.
Patch	Aggiornamento di sicurezza.	La gestione delle patch riduce le vulnerabilità note.

6. Autenticazione e autorizzazione: differenza fondamentale

Questa distinzione è importantissima. Se la capisci, puoi scrivere meglio quasi ogni sezione sulla sicurezza.

Concetto	Domanda	Esempio
Autenticazione	Chi sei?	Mario Rossi inserisce username, password e codice MFA.
Autorizzazione	Cosa puoi fare?	Mario Rossi può vedere le proprie pratiche, ma non modificare quelle di altri cittadini.

Errore comune

Dire 'metto la password e quindi il sistema è sicuro'. La password riguarda solo l'autenticazione. Serve anche autorizzazione: dopo aver capito chi è l'utente, il sistema deve controllare cosa può fare.

Frase pronta

> *L'accesso deve essere gestito tramite autenticazione degli utenti e autorizzazione basata sui ruoli, in modo che ogni soggetto possa accedere solo alle informazioni e alle funzionalità necessarie alle proprie mansioni.*

Esempio pratico in una Pubblica Amministrazione

- Cittadino: consulta solo le proprie pratiche e i propri pagamenti.
- Impiegato comunale: gestisce pratiche del proprio ufficio.
- Dirigente: consulta report e indicatori, ma non modifica dati tecnici senza motivo.
- Amministratore di sistema: gestisce utenti e configurazioni, con privilegi controllati e tracciati.

7. Traccia del Giorno 3

> **Traccia**
> Il candidato descriva le principali problematiche di sicurezza informatica nella gestione di un sistema informativo di una Pubblica Amministrazione o di un'infrastruttura critica. Si discutano minacce, vulnerabilità, tecnologie di protezione, gestione degli incidenti, continuità operativa e responsabilità professionali dell'ingegnere.

Questa traccia è sede-neutrale: può essere adattata a Campus, Sapienza, Tor Vergata o Roma Tre. Per renderla concreta scegliamo un esempio semplice: il portale digitale di un Comune.

Esempio concreto scelto

```
Sistema informativo di un Comune:
- servizi anagrafici online
- pagamenti
- prenotazioni
- protocolli e pratiche amministrative
- accesso per cittadini, impiegati e amministratori
```

Questo esempio funziona bene perché contiene dati personali, utenti diversi, servizi pubblici e bisogno di continuità. Non serve conoscere tutta la PA: basta ragionare su dati, accessi, servizi e rischi.

8. Come leggere la traccia senza bloccarti

Quando la traccia parla di sicurezza, non partire da firewall o crittografia. Parti da quattro domande.

Domanda	Risposta nel nostro esempio
Che cosa devo proteggere?	Dati personali dei cittadini, servizi online, credenziali, database, pratiche amministrative.
Da quali problemi?	Phishing, malware, ransomware, accessi abusivi, errori umani, indisponibilità del servizio.
Con quali misure?	Ruoli, MFA, cifratura, firewall, backup, patch, log, monitoraggio, formazione.
Cosa succede se qualcosa va storto?	Si attivano risposta agli incidenti, ripristino da backup, comunicazione e analisi delle cause.

Schema mentale

Prima asset, poi minacce, poi contromisure, poi gestione dell'incidente. Questo è il cuore della risposta.

In una riga

La sicurezza informatica non è una singola tecnologia, ma un insieme coordinato di misure tecniche, organizzative e procedurali per ridurre il rischio.

9. Template da usare oggi

Per una traccia di cybersecurity useremo questo ordine. È una variante del template generale, ma più adatta a sicurezza e rischio.

Punto	Cosa scrivere	Domanda guida
1. Introduzione	Presenta il problema della sicurezza.	Perché il sistema va protetto?
2. Contesto	Descrivi il sistema scelto.	È una PA, un'azienda, un ospedale, un'infrastruttura?
3. Asset	Indica cosa proteggere.	Dati, servizi, applicazioni, account?
4. Minacce	Descrivi i principali pericoli.	Phishing, malware, ransomware, DDoS, errori?
5. Requisiti di sicurezza	Collega a riservatezza, integrità, disponibilità.	Che qualità deve avere il sistema?
6. Contromisure	Proponi misure concrete.	Autenticazione, ruoli, cifratura, firewall, backup, log?
7. Incident response	Spiega come reagire ai problemi.	Come rilevo, contengo e ripristino?
8. Responsabilità	Ruolo dell'ingegnere.	Come progetto, documento e controllo?
9. Conclusione	Chiudi con beneficio e senso della soluzione.	Perché la proposta è credibile?

10. Scaletta pronta della risposta

Prima di scrivere il tema completo, devi sempre fare una scaletta. Questa è già pronta. Puoi usarla quasi uguale all'esame.

```
1. Introduzione:
La sicurezza informatica è essenziale perché il sistema tratta dati e servizi critici.

2. Contesto:
Esempio: sistema informativo di un Comune / PA.

3. Asset:
Dati personali, credenziali, database, servizi online, documenti amministrativi.

4. Minacce:
Phishing, malware, ransomware, accessi non autorizzati, DDoS, errori umani.

5. Obiettivi di sicurezza:
Riservatezza, integrità, disponibilità.

6. Contromisure:
Autenticazione, autorizzazione, MFA, cifratura, firewall, backup, logging, patch.

7. Incident response:
Rilevamento, contenimento, ripristino, comunicazione, analisi post-incidente.

8. Ruolo dell'ingegnere:
Progettare misure adeguate, documentare, valutare i rischi, garantire conformità.

9. Conclusione:
Un sistema sicuro migliora fiducia, continuità e qualità del servizio.
```

Nota per la memoria

Se non ti viene in mente nulla, scrivi almeno: dati da proteggere, minacce, ruoli, cifratura, backup, log, risposta agli incidenti. È già una risposta con struttura.

11. Risposta svolta - versione da esame

Di seguito trovi una risposta completa, non da imparare a memoria. Leggila per capire come si passa dai concetti alla scrittura.

La sicurezza informatica rappresenta un aspetto fondamentale nella progettazione e gestione di un sistema informativo, soprattutto quando il sistema tratta dati personali, servizi pubblici o informazioni strategiche. Un esempio significativo è il portale digitale di una Pubblica Amministrazione, utilizzato da cittadini, dipendenti e amministratori per consultare pratiche, effettuare pagamenti, gestire documenti e accedere a servizi online.

Il primo passo consiste nell'individuare gli asset da proteggere. In questo caso rientrano tra gli asset il database contenente i dati personali dei cittadini, le credenziali degli utenti, le applicazioni web, i server, i documenti amministrativi e la disponibilità dei servizi online. La protezione di tali elementi deve garantire riservatezza, integrità e disponibilità delle informazioni.

Le principali minacce possono essere di natura tecnica o organizzativa. Tra queste si possono citare phishing, malware, ransomware, accessi non autorizzati, attacchi di tipo denial of service, errori umani, configurazioni errate e mancato aggiornamento dei sistemi. Tali minacce possono provocare perdita di dati, interruzione dei servizi, danni economici, danni reputazionali e violazioni normative.

Per ridurre il rischio è necessario adottare misure di sicurezza multilivello. L'accesso deve essere gestito tramite autenticazione sicura, possibilmente con autenticazione a più fattori per gli utenti con privilegi elevati. L'autorizzazione deve essere basata sui ruoli, in modo che ogni utente possa accedere solo alle informazioni e alle funzionalità necessarie. Le comunicazioni devono essere protette tramite HTTPS e i dati sensibili devono essere gestiti secondo criteri di cifratura e minimizzazione.

A livello infrastrutturale possono essere utilizzati firewall, sistemi di rilevamento delle intrusioni, segmentazione degli ambienti, gestione delle patch e monitoraggio continuo. È inoltre importante predisporre backup periodici, testati e separati dall'ambiente principale, così da poter ripristinare il servizio in caso di guasto, attacco ransomware o perdita accidentale di dati.

Un sistema sicuro deve prevedere anche procedure di gestione degli incidenti. In caso di evento anomalo occorre rilevare il problema, contenerne gli effetti, ripristinare i servizi, analizzare le cause e documentare l'accaduto. I log delle operazioni sono fondamentali per garantire tracciabilità, audit e ricostruzione degli eventi.

Il ruolo dell'ingegnere è quello di progettare una soluzione proporzionata ai rischi, considerando non solo gli aspetti tecnici ma anche quelli organizzativi, normativi e di continuità operativa. È inoltre necessario formare gli utenti, poiché molte vulnerabilità derivano da comportamenti errati o scarsa consapevolezza.

In conclusione, la sicurezza informatica di un sistema informativo pubblico deve essere affrontata in modo integrato, combinando tecnologie, procedure, controllo degli accessi, protezione dei dati e capacità di risposta agli incidenti. Solo così è possibile garantire servizi affidabili, proteggere i cittadini e mantenere la fiducia nell'amministrazione digitale.

12. Perché questa risposta funziona

La risposta funziona perché non elenca strumenti a caso. Segue un ordine: problema, contesto, asset, minacce, obiettivi, misure, incidenti, ruolo dell'ingegnere, conclusione.

Parte della risposta	Perché è utile
Introduzione	Fa capire subito che il tema è la protezione di dati e servizi.
Esempio concreto	Evita una risposta astratta e rende il ragionamento credibile.
Asset	Mostra che sai individuare cosa va protetto.
Minacce	Dimostra consapevolezza dei rischi.
Contromisure	Trasforma il problema in soluzione tecnica.
Incident response	Fa vedere che pensi anche a cosa succede dopo un problema.
Ruolo dell'ingegnere	Collega il tema alla professione e alla responsabilità.
Conclusione	Chiude il ragionamento senza lasciare il tema sospeso.

La frase più importante

> *La sicurezza non deve essere vista come un'aggiunta finale, ma come un requisito progettuale da considerare fin dalle prime fasi di analisi del sistema.*

13. Versione breve da 10-12 righe

Questa è la forma che devi riuscire a produrre tu. Non è lunga, ma contiene tutti i pezzi essenziali.

Mini-risposta modello

La sicurezza informatica di un sistema informativo pubblico è fondamentale perché il sistema tratta dati personali e offre servizi essenziali ai cittadini. Gli asset da proteggere sono database, credenziali, applicazioni, server e documenti amministrativi. Le principali minacce includono phishing, malware, ransomware, accessi non autorizzati, errori umani e attacchi finalizzati a rendere indisponibile il servizio. Gli obiettivi di sicurezza sono riservatezza, integrità e disponibilità. Per raggiungerli è necessario adottare autenticazione sicura, autorizzazione basata sui ruoli, cifratura delle comunicazioni, firewall, aggiornamenti periodici, backup e tracciamento tramite log. È importante anche prevedere procedure di risposta agli incidenti, con rilevamento, contenimento, ripristino e analisi delle cause. Il ruolo dell'ingegnere è progettare misure proporzionate ai rischi, documentare le scelte e garantire continuità operativa. In conclusione, una corretta gestione della cybersecurity aumenta l'affidabilità del servizio e protegge utenti, dati e amministrazione.

Schema invisibile della mini-risposta

```
1. Perché serve sicurezza
2. Cosa proteggo
3. Da cosa mi difendo
4. Obiettivi RID
5. Misure tecniche
6. Incidenti e backup
7. Ruolo dell'ingegnere
8. Conclusione
```

14. Frasi pronte da usare all'esame

Usale come mattoni. Non devi usarle tutte, ma devi saperle adattare.

Uso	Frase
Introduzione	La sicurezza informatica deve essere considerata un requisito progettuale fondamentale, soprattutto nei sistemi che trattano dati personali o servizi critici.
Asset	Il primo passo consiste nell'individuare gli asset da proteggere, come dati, applicazioni, credenziali, server e servizi erogati agli utenti.
RID	Gli obiettivi principali sono riservatezza, integrità e disponibilità delle informazioni e dei servizi.
Ruoli	L'autorizzazione basata sui ruoli permette di limitare le operazioni consentite a ciascun utente, riducendo il rischio di accessi impropri.
Cifratura	Le comunicazioni devono essere protette tramite protocolli sicuri, mentre i dati sensibili devono essere gestiti con criteri di cifratura e minimizzazione.
Backup	Backup periodici e testati sono essenziali per garantire il ripristino del servizio in caso di guasto, errore o attacco ransomware.
Log	Il logging consente di tracciare le operazioni, individuare anomalie e ricostruire gli eventi in caso di incidente.
Incidenti	La gestione degli incidenti richiede rilevamento, contenimento, ripristino, comunicazione e analisi delle cause.
Ingegnere	L'ingegnere ha la responsabilità di progettare soluzioni proporzionate ai rischi, documentare le scelte e verificare l'efficacia delle misure adottate.
Conclusione	Una corretta strategia di cybersecurity migliora affidabilità, continuità operativa e fiducia degli utenti nel sistema.

15. Associa minaccia e protezione

Questo esercizio ti aiuta a fissare. Devi imparare a passare da problema a contromisura.

Minaccia/problema	Cosa può causare	Misure da citare
Phishing	Furto di credenziali tramite email ingannevoli.	Formazione utenti, MFA, filtri email, verifica accessi anomali.
Ransomware	Cifratura o blocco dei dati con richiesta di riscatto.	Backup offline/testati, patch, antivirus/EDR, segmentazione, formazione.
Password deboli	Accessi non autorizzati.	Policy password, MFA, hashing password, controllo tentativi.
DDoS	Indisponibilità del servizio.	Sistemi anti-DDoS, ridondanza, monitoraggio, piani di continuità.
Software non aggiornato	Sfruttamento di vulnerabilità note.	Patch management, inventario sistemi, monitoraggio vulnerabilità.
Errore umano	Cancellazione dati, invio a destinatario errato, configurazioni sbagliate.	Procedure, formazione, backup, controllo privilegi, log.

Come usarla nella risposta

Non devi descrivere tutti gli attacchi. Scegline 3 o 4 e collega sempre una misura di protezione. Questo basta per dimostrare ragionamento.

16. Esercizio guidato: completa le frasi

Prima di scrivere la tua risposta, completa mentalmente queste frasi. Se vuoi, puoi copiarle su un foglio e riempire gli spazi.

1. Il sistema che scelgo come esempio è _____.
2. Gli asset principali da proteggere sono _____.
3. Le minacce più rilevanti sono _____.
4. Gli obiettivi di sicurezza sono _____.
5. Per controllare gli accessi userei _____.
6. Per proteggere i dati userei _____.
7. Per garantire disponibilità e ripristino servono _____.
8. In caso di incidente occorre _____.
9. Il ruolo dell'ingegnere è _____.
10. In conclusione, il sistema risulta _____.

Esempio di completamento

1. portale digitale di un Comune
2. dati personali, credenziali, database, applicazioni e documenti
3. phishing, ransomware, accessi abusivi, errori umani e DDoS
4. riservatezza, integrità e disponibilità
5. autenticazione, MFA e autorizzazione basata sui ruoli
6. HTTPS, cifratura, minimizzazione dei dati e log
7. backup, ridondanza, monitoraggio e piano di continuità
8. rilevare, contenere, ripristinare e analizzare le cause
9. progettare misure proporzionate ai rischi e documentarle
10. più affidabile, sicuro e utilizzabile dagli utenti

17. Costruzione passo passo della tua risposta

Ora trasformiamo lo schema in testo. Ti do una traccia semi-guidata. Tu devi sostituire o completare alcune parti.

```
La sicurezza informatica di un _____ è fondamentale perché il sistema
tratta _____ e offre _____.

Gli asset da proteggere sono _____, _____ e
_____.

Le principali minacce includono _____, _____ e
_____.

Gli obiettivi di sicurezza sono riservatezza, integrità e disponibilità.

Per ridurre il rischio è opportuno adottare _____,
_____, _____ e _____.

In caso di incidente è necessario _____, _____ e
_____.

Il ruolo dell'ingegnere è _____.

In conclusione, una corretta gestione della sicurezza permette di
_____.
```

Consiglio pratico

Se non ti viene una frase elegante, scrivila prima in modo grezzo. Poi la ripuliamo. La prima prova richiede ordine e ragionamento, non poesia.

18. Errori da evitare

Errore	Perché è un problema	Come correggerlo
Elencare solo strumenti	Sembra una lista imparata a memoria.	Collega ogni strumento a un rischio: firewall per filtrare, backup per ripristinare, log per tracciare.
Dire solo 'il sistema deve essere sicuro'	È troppo generico.	Specifica riservatezza, integrità e disponibilità.
Confondere autenticazione e autorizzazione	È un errore concettuale comune.	Autenticazione = chi sei. Autorizzazione = cosa puoi fare.
Dimenticare la disponibilità	La sicurezza non è solo segretezza.	Parla anche di backup, continuità operativa e risposta agli incidenti.
Ignorare le persone	Molti incidenti partono da errori umani.	Cita formazione, procedure e consapevolezza degli utenti.
Usare termini troppo avanzati senza spiegarli	Rende la risposta fragile.	Meglio pochi concetti chiari e applicati a un esempio concreto.

Frase salva-risposta

> *La sicurezza deve essere affrontata con un approccio multilivello, combinando misure tecniche, organizzative e procedurali proporzionate ai rischi del sistema.*

19. Collegamento leggero alle prove successive

La priorità resta la prima prova. Però questo argomento ti aiuterà anche dopo, senza studiare altro adesso.

Prova	Come torna utile
Prima prova	Tema discorsivo su cybersecurity, sicurezza, qualità, sistemi informativi, PA, infrastrutture critiche.
Seconda prova	Possibile approfondimento tecnico su architettura sicura, database, accessi, cloud, logging, backup.
Prova pratica	Schema di sistema con frontend, backend, database, firewall, IAM, backup, log, monitoraggio.
Orale	Domande su responsabilità dell'ingegnere, protezione dati, continuità operativa, incidenti e scelte progettuali.

Non approfondire ora

Non devi studiare crittografia matematica, protocolli di rete avanzati o normative nel dettaglio. Per ora devi saper scrivere una risposta credibile e ordinata.

20. Mini-schema architetturale da citare

Quando la traccia chiede anche come proteggere un sistema, puoi descriverlo così. Non è un disegno tecnico completo, ma una struttura mentale utile.

```
Utente
|
| autenticazione + MFA
v
Frontend web / portale
|
| HTTPS
v
Backend applicativo
|
| controlli di autorizzazione + log
v
Database
|
| backup + cifratura + replica
v
Sistema di monitoraggio / risposta incidenti
```

Come spiegarlo

Il frontend consente l'accesso degli utenti. Il backend applicativo applica le regole di autorizzazione e registra le operazioni. Il database conserva i dati in modo strutturato e deve essere protetto tramite backup, cifratura e controllo degli accessi. Il monitoraggio consente di rilevare anomalie e incidenti.

21. Sistema per fissare: A-M-R-C-I

Per non dimenticare l'ordine della risposta usa questa sigla:

Lettera	Parola	Domanda
A	Asset	Cosa devo proteggere?
M	Minacce	Da cosa devo difendermi?
R	Rischi	Che danno può accadere?
C	Contromisure	Con quali misure riduco il rischio?
I	Incidenti	Cosa faccio se il problema accade davvero?

Da ripetere a voce

Asset, minacce, rischi, contromisure, incidenti.

Poi aggiungo: responsabilità dell'ingegnere e conclusione.

Versione ancora più breve

```
Proteggo COSA?
Da COSA?
Con COSA?
E se succede, COSA FACCIO?
```

22. Mini-esercizio finale da mandarmi

Adesso scrivi una risposta di 10-12 righe. Non cercare di essere originale. Usa lo schema. Io poi la correggo per chiarezza, completezza e stile da esame.

> **Consegna**
> Scrivi una mini-risposta alla traccia: sicurezza informatica di un sistema informativo pubblico o di una infrastruttura critica.

Schema obbligatorio

```
1. La sicurezza informatica è importante perché...
2. Il sistema preso come esempio è...
3. Gli asset da proteggere sono...
4. Le principali minacce sono...
5. Gli obiettivi di sicurezza sono...
6. Per controllare gli accessi si usano...
7. Per proteggere dati e comunicazioni si usano...
8. Per garantire continuità operativa servono...
9. In caso di incidente bisogna...
10. Il ruolo dell'ingegnere è...
11. In conclusione...
```

Parole che devi provare a usare

- riservatezza
- integrità
- disponibilità
- autenticazione
- autorizzazione basata sui ruoli
- cifratura
- backup
- log
- risposta agli incidenti

23. Pagina finale del Giorno 3

Cosa devi ricordare

- Cybersecurity significa proteggere dati, sistemi e servizi da accessi non autorizzati, errori, guasti e attacchi.
- Gli obiettivi principali sono riservatezza, integrità e disponibilità.
- La risposta deve partire dagli asset, non dagli strumenti.
- Autenticazione = chi sei; autorizzazione = cosa puoi fare.
- Backup e risposta agli incidenti servono perché nessun sistema è sicuro al 100%.
- L'ingegnere deve progettare misure proporzionate ai rischi e documentare le scelte.

Template finale

```
Introduzione
Contesto
Asset
Minacce
Obiettivi RID
Contromisure
Incident response
Ruolo dell'ingegnere
Conclusione
```

Obiettivo del Giorno 3

Non diventare esperto di cybersecurity, ma saper scrivere una risposta ordinata, concreta e credibile. Se riesci a seguire il template e a usare 5-6 parole chiave in modo corretto, la giornata è riuscita.

Quando hai scritto la tua mini-risposta, incollamela in chat. La correggerò su tre aspetti: chiarezza, completezza, stile da esame.