1) Cosa si intende per "data breach"?
2) Come si deve comportare una PA in caso di un'esfiltrazione di dati ("data breach")?
3) Una delle piattaforme abilitanti inserite nel Piano Triennale per l'Informatica nella PA è PagoPA. Cosa è?
4) Descrivere in che cosa consiste SPID.
5) Quali sono i vantaggi per cittadini imprese e PA nell'adozione di SPID (Sistema Pubblico Identità Digitale) ?.
6) Cos'è il Responsabile per la Transizione Digitale secondo l'art.17 del CAD ?
7) Cos'è il DPO secondo il GDPR e che funzioni ha ?
8) Che differenza c'è tra firma PAdES e CAdES?
9) Spiegare la differenza tra Firma Elettronica Semplice e Qualificata.
10) Cosa si intende per trasparenza nella pubblica amministrazione?
11) Cosa si intende per Competenze Digitali secondo quanto previsto nell'Agenda Digitale del Veneto 2025?
12) Cosa si intende per Infrastrutture secondo quanto previsto nell'Agenda Digitale del Veneto 2025?
13) Cosa si intende per Dati secondo quanto previsto nell'Agenda Digitale del Veneto 2025?
14) Cosa si intende per Servizi Digitali secondo quanto previsto nell'Agenda Digitale del Veneto 2025?
15) In cosa consistono le Misure minime di sicurezza ICT per le pubbliche amministrazioni di AGID?
16) Cosa prevede il GDPR in merito alla gestione delle password ?
17) Cosa significa sviluppare un software security by design ?
18) Cosa significa sviluppare un software privacy by design ?
19) Qual'è la differenza tra titolare e responsabile del trattamento dei dati ?
20) Che cosa si intende per Accessibilità dei siti web, fare alcuni esempi.
21) Confidenzialità, Integrità e Disponibilità sono tre principi cardine del GDPR nel contesto della sicurezza dell'informazione, il candidato li descriva brevemente.
22) Cos'è la valutazione d'impatto della protezione dei dati (DPIA)?
23) E' sempre obbligatoria la valutazione d'impatto della protezione dei dati (DPIA)?

1. Regularly updating your software and operating systems is a fundamental practice in maintaining cybersecurity resilience.
2. Multi-factor authentication adds an extra layer of security by requiring multiple forms of verification for access.
3. Continuous monitoring of network traffic helps identify suspicious activities and enables swift responses to potential security incidents.
4. Educating employees on cybersecurity best practices is essential for creating a culture of awareness and responsibility.
5. When establishing a password management policy, it is important to consider several key factors to ensure a balance between security and convenience.
6. Through the implementation of cloud computing, our organization has significantly enhanced its scalability and resource management capabilities.
7. Utilizing advanced machine learning algorithms, the cybersecurity software can proactively identify and mitigate potential threats.
8. Adopting a microservices architecture has enabled our software applications to be more modular, scalable, and independently deployable.
9. Employing DevOps practices has streamlined our software development lifecycle, fostering collaboration between development and operations teams.
10. Conducting regular vulnerability assessments and penetration testing is imperative to identify and address potential security loopholes in our IT infrastructure.
11. In response to emerging cybersecurity threats, the organization implemented a multifaceted approach, combining firewalls, intrusion detection systems, and regular security audits.
12. The implementation of a distributed version control system like Git has improved collaboration among developers, allowing for parallel development and efficient code merging.
13. Employing biometric authentication methods, such as fingerprint recognition and facial scanning, enhances the security of access control systems.
14. Remote management tools enable administrators to monitor and control data center operations from a distance.
15. Redundant data storage systems prevent data loss in case of hardware failures in the data center.
16. The data center employs encryption protocols to secure data during transmission and storage.
17. The data center's disaster recovery plan includes off-site backups to protect against on-site data loss.
18. Regular audits are conducted to assess and enhance the physical and cyber security of the data center.
19. Continuous delivery practices empower development teams to deliver software updates frequently, ensuring rapid responses to changing user requirements.
20. Automated testing frameworks, when implemented thoughtfully, contribute to software development efficiency by reducing manual testing efforts and improving code quality.
21. Load balancing mechanisms distribute network traffic across multiple servers, ensuring optimal performance and preventing individual servers from becoming overwhelmed.
22. Hybrid cloud architectures leverage a combination of on-premises servers and cloud services, providing flexibility and scalability to organizations.
23. The implementation of secure socket layer (SSL) certificates on web servers ensures the encryption of data transmitted between the server and clients, enhancing security.

1. Cosa si intende per "autenticazione a due fattori" e quali sono i vantaggi in termini di sicurezza?
2. Spiega il concetto di "firewall" e come può contribuire a proteggere una rete informatica.
3. Descrivi il concetto di "patch management" e l'importanza di tenere aggiornati i software.
4. Cosa significa "backup" e perché è importante per la sicurezza dei dati?
5. Cos'è il "social engineering" in termini di sicurezza informatica?
6. Cosa significa "HTTPS" quando si naviga su Internet?
7. Cosa significa "criptografia"?
8. Quando si ricorre ad analizzare i log generati dalle applicazioni?
9. A cosa serve uno strumento di monitoraggio delle applicazioni?
10. Cosa si intende per repository?
11. Quando si parla di specifiche architetturali di un'applicativo a cosa si fa riferimento?
12. Qual'è il concetto di "load balancing" e come può migliorare le prestazioni di un server?
13. Qual'è la differenza tra la gestione on premise e la gestione in cloud?
14. Cosa si intende per sistema di autenticazione?
15. Cosa si intende per profilazione in ambito applicativo?
16. Quale tra le seguenti tecnologie a banda larga è considerata più veloce? Fiber To The Cabinet, Fiber To The Home, Fixed Wireless Access (FTTC, FTTH, FWA)
17. I sistemi informativi della PA, per poter offrire adeguati servizi, a certe categorie di utenti, hanno talvolta bisogno di utilizzare sistemi GIS: che cosa sono ?
18. In un Database, come è possibile ridurre il tempo di accesso ad un record?
19. Per garantire la continuità operativa in un Datacenter, quali soluzioni si possono adottare ?
20. Quale frequenza, tra i 2.5 e 5 Ghz, sceglierebbe, per attivare una rete WIFI meno soggetta a disturbi generati dagli ostacoli ?
21. Quale frequenza, tra i 2.5 e 5 Ghz, sceglierebbe, per attivare una rete WIFI più performante ?
22. Cosa si intende per applicazione Client/Server?
23. Nell'ambito del Cloud Computing, che tipo di applicazione è Gmail di Google?
24. Cosa fa la seguente istruzione SQL: DELETE FROM Clienti where città ="Venezia"?
25. Cosa fa la seguente istruzione SQL: SELECT * FROM Clienti where città ="Venezia"?
26. Cosa fa la seguente istruzione SQL: SELECT Nome,Cognome FROM Clienti where città ="Venezia"»?
27. Cosa si intende per Sigle Sign-On? Illustri i vantaggi di tale paradigma informatico.
28. Che differenza c'è tra il protocollo http ed https?
29. Ogni quanto tempo devono essere aggiornate le password su un applicativo che tratta dati sensibili?
30. Che cos'e CryptoLocker?
31. Che cos'è un Ransomware ?
32. Cosa si intende per Business Continuity ?
33. Cosa si intende per Disaster Recovery ?
34. Cosa si intende per Internet delle cose (IoT)?
35. Cosa significa il termine "multitenancy" nel cloud computing?
36. Come può essere utilizzata l'intelligenza Artificiale nella pubblica amministrazione?
37. Cos'è un sistema di anti SPAM e come funziona ?
38. Che cosa si intende per Web Collaboration all'interno di un contesto Aziendale ?
39. Cosa si intende per "sistema di trouble ticketing"?
40. Che cosa sono le FAQ e qual'è il loro ruolo in una piattaforma online?
41. Qual è il ruolo principale di un bilanciatore di carico in un'architettura di rete e come contribuisce a migliorare le prestazioni e l'affidabilità del sistema?
42. Cosa si intende per "protezione perimetrale" di una rete informatica ?

43. Qual è l'obiettivo principale di condurre un Penetration Test nell'ambito della sicurezza di una rete informatica aziendale
44. Cosa si intende per virtualizzazione di un server ?