Domanda A. Sicurezza Informatica

1) Cosa si intende per autenticazione a 2 fattori e quali valutazioni costi/benefici debbono essere fatte per attivarlo ad esempio per l'accesso al sistema di posta elettronica dell'Ente
2) Cosa si intende per VPN e quali sono gli aspetti relativi alla sicurezza informatica
3) Elencare le principali cause che possono incidere negativamente sulla sicurezza del sistema informativo di una organizzazione
4) Cos'è un "ransomware" e come ci si difende?
5) Quali problematiche relative alle sicurezza informatica deve porsi un amministratore di sistema, rispetto alla gestione della posta elettronica di un Ente?
6) Rispetto alla sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle PA, così come definite dall'Art. 51 del cad, si descrivano le linee guida e i riferimenti normativi da seguire nell'ambito della gestione della sicurezza informatica.
7) Dotando l'Ente di un firewall, quali elementi di prevenzione del rischio si ottengono, dovendo preoccuparsi della sicurezza informatica di un Ente?
8) Quali sono gli aspetti di sicurezza informatica che vanno valutati nella scelta di un nuovo software applicativo?
9) Quali accorgimenti si devono prendere se si devono salvare dati personali su dispositivi portatili o memorie rimovibili?
10) Che cos'è il "phishing" e come ci si difende?

Domanda B. CAD – AGID

1) Visto l'art. 3-bis (sezione II) e l'art.64 (sezione III) del Codice per l’Amministrazione Digitale (CAD), cosa si intende per identità digitale?
2) Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile?
3) Visto l'art. 5 (sezione II) del Codice per l’Amministrazione Digitale (CAD), cosa si intende per 'pagamenti con modalità informatiche'? come viene realizzato nel concreto?
4) Visto l'art. 1 del Codice per l’Amministrazione Digitale (CAD), cosa si intende per 'formato aperto' e 'dati di tipo aperto' e come li tratta la PA
5) Visto l'art. 6-ter del Codice per l’Amministrazione Digitale (CAD) cosa si intende per 'Indice dei domicili digitali delle pubbliche amministrazioni'
6) Visto l'art. 17 del Codice per l’Amministrazione Digitale (CAD) cosa si intende per 'Responsabile per la transizione digitale'
7) Visto l'art. 24 del Codice per l’Amministrazione Digitale (CAD) cosa si intende per 'Firma digitale'
8) Visto gli art. 43 e 44 del Codice per l’Amministrazione Digitale (CAD) cosa si intende per 'Conservazione dei documenti informatici'
9) Visto l'art. 48 del Codice per l’Amministrazione Digitale (CAD)cosa si intende per 'PEC'?
10) Cos’è un documento analogico e come posso produrre una copia digitale di un documento analogico?

Domanda C – TUEL

1) Il ruolo e le competenze dei consigli degli EE.LL.
2) Caratteristiche e differenze tra delibere e determinazioni.
3) Gli organi di governo della Provincia con particolare riferimento alla loro elezione, ai sensi della L.56/2014.
4) Le differenze tra gli organi di governo delle province e dei comuni.
5) Le funzioni fondamentali dei Comuni.
6) Le funzioni fondamentali delle Province, ai sensi della L. 56/2014.
7) Il principio di separazione tra organi di governo e organi di gestione.
8) Il candidato illustri gli elementi fondamentali dell'impegno di spesa.
9) Gli strumenti di programmazione degli enti locali.
10) Il candidato illustri i compiti del dirigente degli EE.LL.

Inglese

1) Our system has detected an unusual rate of unsolicited mail originating from your IP address. To protect our users from spam, mail sent from your IP address has been temporarily blocked. For more information, visit 'Prevent mail to Gmail users from being blocked or sent to spam.
2) Multi-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).
3) A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN).
4) In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
5) As of 2020, phishing is by far the most common attack performed by cybercriminals, the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.
6) As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory.
7) All matters concerning PEC in Italy are supervised and regulated by a special government agency called AgID which determines the authorized certified email providers, the legal framework of PEC and the rules and terms of use.
8) Spamming is the use of messaging systems to send multiple unsolicited messages (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, for any prohibited purpose (especially the fraudulent purpose of phishing), or simply repeatedly sending the same message to the same user.
9) A hacker is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means. Though the term hacker has become associated in popular culture with a security hacker, hacking can also be utilized by legitimate figures in legal situations.
10) Computer security, cybersecurity, or information technology security is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.