DOMANDE PROCEDURA VALUTATIVA PER LA PROGRESSIONE TRA LE AREE DEL PERSONALE DIPENDENTE, AI SENSI DEL D.LGS. N. 165/2001, ART. 52, COMMA 1 BIS E DELL'ART. 13, COMMA 6 DEL CCNL FUNZIONI LOCALI 2019-2021, PER COMPLESSIVI N. 153 POSTI DELL'AREA DEGLI ISTRUTTORI E DELL'AREA DEI FUNZIONARI E DELL'ELEVATA QUALIFICAZIONE, IN VARI PROFILI, PRESSO I DIPARTIMENTI E LA SEGRETERIA GENERALE DELLA GIUNTA REGIONALE - CANDIDATI APPARTENENTI ALL'AREA DEGLI ISTRUTTORI - PROVA PROVA A RISPOSTA MULTIPLA - BUSTA 3_D/IT

---

1) **Ai sensi dell'art. 1, comma 44 della legge n. 190/2012 la violazione dei doveri contenuti nel codice di comportamento, compresi quelli relativi all'attuazione del Piano di prevenzione della corruzione:**

A comporta una sanzione amministrativa pecuniaria
B è fonte di responsabilità disciplinare
C non ha conseguenze disciplinari

---

2) **Ai sensi dell'art. 1, comma 46 della legge n. 190/2012, coloro che sono stati condannati, anche con sentenza non passata in giudicato, per i reati previsti nel capo I del titolo II del libro secondo del codice penale:**

A non possono fare parte, anche con compiti di segreteria, di commissioni per l'accesso o la selezione a pubblici impieghi
B possono fare parte, anche con compiti di segreteria, di commissioni per l'accesso o la selezione a pubblici impieghi
C devono fare parte, anche con compiti di segreteria, di commissioni per l'accesso o la selezione a pubblici impieghi

---

3) **Ai sensi dell'art. 1, comma 28 della legge n. 190/2012 le amministrazioni provvedono al monitoraggio periodico del rispetto dei tempi procedimentali:**

A attraverso la tempestiva eliminazione delle anomalie
B attraverso verifiche a campione
C attraverso l'eliminazione delle anomalie all'inizio di ogni legislatura

---

4) **Ai sensi dell'art. 43, comma 4, del D. Lgs. 33/13 e ss.mm.ii., chi controlla ed assicura la regolare attuazione dell'accesso civico?**

A i dirigenti responsabili dell'amministrazione e il responsabile per la trasparenza
B l'organo politico
C il responsabile per la trasparenza

---

5) **Ai sensi dell'art. 10 del D. Lgs. 33/13 e ss.mm.ii., ogni amministrazione, in un'apposita sezione del Piano triennale per la prevenzione della corruzione, indica:**

A i responsabili della trasmissione e della pubblicazione dei documenti, delle informazioni e dei dati
B i responsabili dei singoli uffici tecnici
C i responsabili degli uffici dell'amministrazione

---

6) **Ai sensi dell'art. 7 del D. Lgs. 33/13 e ss.mm.ii., i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria, resi disponibili anche a seguito dell'accesso civico, sono pubblicati in formato di tipo:**

A aperto, ma non sono riutiizzabili
B aperto e sono riutiizzabili senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità
C chiuso

7) **A norma dell'art. 35, comma 2, della Legge regionale 30/07/2021, n. 18, il Comitato unico di garanzia per le pari opportunità, la valorizzazione del benessere di chi lavora e contro le discriminazioni, da chi è formato?**

A è formato da un componente per ciascuna delle organizzazioni sindacali e da un numero di rappresentanti dell'amministrazione regionale non inferiore a due unità
B è formato in maniera paritetica da un componente per ciascuna delle organizzazioni sindacali maggiormente rappresentative a livello di amministrazione regionale e da un pari numero di rappresentanti dell'amministrazione regionale
C è formato da componenti per ciascuna delle organizzazioni sindacali in numero proporzionale alla rappresentatività nell'amministrazione regionale e da un pari numero di rappresentanti dell'amministrazione regionale

---

8) **A norma dell'art. 36, comma 6, della Legge regionale 30/07/2021, n. 18, chi approva il piano triennale delle attività formative del personale dipendente?**

A il dirigente della struttura regionale competente in materia di formazione del personale
B il direttore di dipartimento
C La Giunta regionale

---

9) **A norma dell'art. 13, comma 4, della Legge regionale 30/07/2021, n. 18, nel caso in cui le attività di competenza dei dirigenti di direzione coinvolgano più strutture, da chi sono fissati gli indirizzi e le modalità?**

A dal segretario generale
B dalla giunta regionale
C dal direttore di dipartimento

---

10) **Le sentenze passate in giudicato che accolgono il ricorso proposto avverso il silenzio inadempimento dell'amministrazione sono trasmesse, in via telematica,**

A al Ministero dell'Interno
B alla Corte dei conti.
C alla presidenza del Consiglio dei ministri

---

11) **Chi può chiedere, in fase di istruttoria del procedimento amministrativo, il rilascio di dichiarazioni, la rettifica di dichiarazioni o istanze erronee o incomplete (art. 6, legge n. 241/1990)?**

A Non è possibile chiedere dichiarazioni di rettifica di instanze erronee o incomplete
B Il responsabile del procedimento
C L'organo di indirizzo politico-amministrativo dell'Amministrazione

---

12) **A chi spetta, ai sensi della legge n. 241/90, l'adozione del provvedimento finale nel procedimento amministrativo?**

A Al Dirigente
B Al Responsabile del procedimento che è sempre competente
C Al responsabile del procedimento che ne abbia la competenza ovvero all'organo competente per l'adozione

---

13) **L'art. 12 della legge 241/1990 subordina la concessione di contributi, sussidi o vantaggi economici:**

A Alla predeterminazione di criteri e modalità alle quali le amministrazioni si attengono
B Alla esclusiva presentazione di valida richiesta da parte del richiedente
C Alla esclusiva predeterminazione di criteri e alla disponibilità finanziaria

---

14) **Il responsabile del provvedimento finale, qualora ravvisi di trovarsi in conflitto d'interessi, in base all'art. 6-bis della 241/1990, deve:**

A Adottare il provvedimento finale evidenziando nel dispositivo la sua situazione di conflitto d'interessi
B Astenersi, segnalando ogni situazione di conflitto, anche potenziale
C Designare un soggetto che lo affianchi a garanzia della correttezza degli atti

---

15) **Ai sensi della legge 241/1990, art.25, nel caso di richiesta di accesso agli atti l'amministrazione:**

A Può comunque rifiutarsi o differire la risposta se ritiene inopportuna la richiesta
B Il rifiuto, il differimento e la limitazione dell'accesso sono ammessi nei casi e nei limiti stabiliti e debbono essere motivati
C Non può rifiutarsi, differire o limitare l'accesso

---

16) **Cosa prevede il "Perimetro di Sicurezza Nazionale"?**

A Controlli su reti e servizi critici
B Sanzioni per cybercrime
C Direttive per la privacy

---

17) **In Italia, la relazione annuale sulla cybersecurity è pubblicata da:**

A AgID
B Ministero dell'Interno
C Agenzia per la Cybersicurezza Nazionale (ACN)

---

18) **Dove è definita la figura del referente per la cybersicurezza?**

A Nel regolamento dell'Agenzia per la cybersicurezza
B Nella legge 90/2024
C Nell'articolo 17 del codice dell'amministrazione digitale

---

19) **Qual è il ruolo dell'Agenzia per la cybersicurezza nazionale (ACN)?**

A Monitorare le minacce e fornire linee guida
B Supervisionare le amministrazioni pubbliche
C Gestire i progetti di digitalizzazione

---

20) **L'estrazione dei domini relativi a rivendicazioni di attacchi riportati nei Data Leak Site è utile al monitoraggio delle minacce ransomware su una constituency di riferimento. In quale fase del ciclo intelligence ci troviamo?**

A Collection & Processing
B Analisys
C Dissemination

---

21) **Quale delle seguenti minacce sfrutta l'ingegneria sociale per ottenere informazioni sensibili, spesso tramite email o messaggi ingannevoli?**

A Phishing
B DDoS
C Malware

---

22) **Un attacco di "spoofing" si verifica quando:**

A Un firewall blocca il traffico legittimo di rete
B Un utente dimentica la propria password e richiede un reset
C Un aggressore simula o falsifica l'identità di un'entità legittima (es. indirizzo IP, indirizzo email, numero di telefono) per ingannare un sistema o un utente

---

23) **Quale è il possibile impatto di un attacco di tipo DDoS?**

A La cifratura di tutti i file del sistema infettato
B La mancata disponibilità di un servizio
C La compromissione delle credenziali di accesso a un sistema

---

24) **La "Business Impact Analysis" (BIA) ha lo scopo di:**

A Identificare le vulnerabilità di rete di un sistema informatico

B Determinare l'impatto potenziale di interruzioni o incidenti su funzioni e processi aziendali critici
C Calcolare il valore di mercato degli asset IT di un'organizzazione

---

25) Qual è il primo passo fondamentale nel processo di gestione del rischio di sicurezza informatica?

A Monitoraggio e revisione
B Identificazione degli asset, delle minacce e delle vulnerabilità
C Implementazione delle contromisure

---

26) Qual è l'obiettivo principale di una strategia di Data Loss Prevention (DLP)?

A Crittografare tutti i dati archiviati sui server
B Bloccare tutti gli attacchi DDoS
C Impedire che informazioni sensibili escano da un'organizzazione in modo non autorizzato

---

27) Quale documento descrive il processo strutturato che un'organizzazione segue per rispondere a un incidente di sicurezza informatica, dalla rilevazione al ripristino completo?

A Acceptable Use Policy
B Incident Response Plan (IRP)
C Privacy Policy

---

28) Qual è il risultato finale atteso di una corretta e completa valutazione del rischio di sicurezza informatica?

A Una lista dettagliata di rischi identificati, classificati in base alla loro probabilità e al potenziale impatto
B L'eliminazione totale e definitiva di tutte le minacce esistenti
C L'acquisto immediato di nuove apparecchiature hardware di sicurezza

---

29) Nel contesto della gestione del rischio, una "vulnerabilità" è definita come:

A Un evento dannoso che può verificarsi
B Una debolezza in un sistema, processo o controllo che può essere sfruttata da una minaccia
C Una contromisura di sicurezza implementata

---

30) Qual è l'obiettivo principale di un Business Continuity Plan (BCP) in relazione alla sicurezza informatica?

A Garantire la ripresa delle operazioni aziendali critiche e il ripristino dei servizi dopo un incidente o un disastro
B Prevenire tutti gli attacchi informatici indistintamente
C Formare il personale sulla sicurezza delle password