UNIVERSITA' DEGLI STUDI ROMA TRE

CONCORSO PUBBLICO, PER ESAMI, A TEMPO INDETERMINATO PER LA COPERTURA DI N. 1 POSTO DI CATEGORIA D, POSIZIONE ECONOMICA 1, AREA AMMINISTRATIVA-GESTIONALE, E N. 1 POSTO DI CATEGORIA D, POSIZIONE ECONOMICA 1, AREA AMMINISTRATIVA-GESTIONALE, RISERVATO, AI SENSI DELL'ART. 52, COMMA 1*BIS* DEL D.LGS. 165/2001, AL PERSONALE A TEMPO INDETERMINATO IN SERVIZIO PRESSO L'UNIVERSITA' DEGLI STUDI ROMA TRE INQUADRATO NELLACATEGORIA C IN POSSESSO DEI REQUISITI PREVISTI PER L'ACCESSO DALL'ESTERNO, PER LE ESIGENZE DELL'AMMINISTRAZIONE CENTRALE DELL'ATENEO (COD. ID. CONCORSO AM1D1AG20)

SECONDA PROVA SCRITTA

4 GIUGNO 2020

1	**Ai sensi dell'art. 1 del d.lgs. n. 33/2013, per trasparenza s'intende:**
a	accessibilità dei documenti detenuti dall'amministrazione dello Stato, nel rispetto della riservatezza e della discrezionalità concernente il perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche
b	accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, nel rispetto del divieto del controllo generalizzato sull'operato della pubblica amministrazione
c	accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche
d	accessibilità dei documenti amministrativi solo per i soggetti che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso
e	accessibilità dei dati e documenti detenuti dalle pubbliche amministrazioni, nel rispetto della ragion di Stato, del segreto amministrativo e della discrezionalità rispetto all'utilizzo delle risorse pubbliche
2	**L'art. 2 del d.lgs. n. 33/2013 stabilisce che le disposizioni del decreto "disciplinano la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni…"**
a	tramite l'accesso documentale e la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione delle pubbliche amministrazioni
b	tramite l'accesso civico e la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione delle pubbliche amministrazioni, ma non la loro attività
c	tramite l'accesso civico e la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni
d	tramite la pubblicazione di documenti, informazioni e dati concernenti l'attività delle pubbliche amministrazioni, ma non la loro organizzazione
e	tramite gli istituti già presenti nella Legge n. 241/1990
3	**Secondo l'art. 3 del d.lgs. n. 33/2013, "Tutti i documenti, le informazioni e i dati oggetto di accesso civico, ivi compresi quelli oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono…"**
a	pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli
b	conoscibili solo dai soggetti che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso
c	pubblici e chiunque ha diritto di conoscerli, ma la fruizione è condizionata al pagamento di una tassa fissata annualmente da ogni amministrazione
d	pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, ma non di utilizzarli e riutilizzarli
e	pubblici, a meno che l'amministrazione non preveda, mediante regolamento, che essi vengano tenuti riservati
4	**Se le amministrazioni non ottemperano all'obbligo di pubblicare documenti e informazioni previsto dalla normativa vigente…**
a	solo coloro che hanno un interesse concreto, diretto e attuale possono richiedere i documenti

	medesimi
b	non può in alcun modo richiedersi la pubblicazione, salvo nei casi stabiliti dal Governo tramite regolamento
c	occorre proporre ricorso al Consiglio di Stato entro 5 giorni dalla scoperta della mancata pubblicazione
d	chiunque ha diritto di richiedere i documenti medesimi, ma il Governo tramite regolamento può escludere determinate categorie di soggetti dall'accesso
e	chiunque ha diritto di richiedere i documenti medesimi
5	**È possibile accedere a dati e documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico?**
a	no, a meno che ciò non sia previsto da una norma di legge o di regolamento
b	no, salvo che per i dati e i documenti detenuti dalle amministrazioni delle regioni e degli enti locali
c	sì, chiunque ne ha diritto
d	sì, ma soltanto a dati e documenti detenuti dalle amministrazioni centrali e periferiche dello Stato
e	sì, ma può richiedere l'accesso soltanto chi abbia un interesse diretto, concreto e attuale a conoscere dati e documenti
6	**Il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di…**
a	cinque giorni dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati
b	dieci giorni dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati
c	trenta giorni dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati
d	sessanta giorni dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati
e	centoventi giorni dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati
7	**Avverso la decisione di diniego totale o parziale dell'accesso o di mancata risposta entro il termine previsto da parte dell'amministrazione competente o, in caso di richiesta di riesame, avverso la decisione di diniego totale o parziale dell'accesso del responsabile della prevenzione della corruzione e della trasparenza, il richiedente può proporre ricorso…**
a	al Consiglio di Stato
b	al Tribunale civile
c	alla Commissione per l'accesso istituita presso la Presidenza del Consiglio dei Ministri
d	alla Corte dei Conti
e	all'Autorità nazionale anticorruzione

8	**Ai sensi dell'art. 5-bis, comma 2, l'accesso civico generalizzato è rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:**
a	la protezione dei dati personali, in conformità con la disciplina legislativa in materia
b	gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali
c	la libera manifestazione del pensiero dei cittadini
d	i diritti dei consumatori, in conformità con la disciplina legislativa in materia
e	l'accesso civico può essere rifiutato solo se il diniego è necessario per evitare un pregiudizio concreto di un interesse pubblico
9	**L'art. 8 del d.lgs. n. 33/2013 stabilisce che i dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali e quanto previsto dagli articoli 14, comma 2, e 15, comma 4, per un periodo di:**
a	6 mesi, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti
b	1 anno, decorrente dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti
c	5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti
d	10 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti
e	20 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti
10	**Ai sensi dell'art. 46 del d.lgs. n. 33/2013, l'inadempimento degli obblighi di pubblicazione previsti dalla normativa vigente, il rifiuto, il differimento e la limitazione dell'accesso civico, al di fuori delle ipotesi previste dall'articolo 5-bis…**
a	costituiscono elemento di valutazione della responsabilità dirigenziale
b	costituiscono elemento di valutazione della responsabilità dirigenziale, ma non costituiscono eventuale causa di responsabilità per danno all'immagine dell'amministrazione
c	costituiscono eventuale causa di responsabilità per danno all'immagine dell'amministrazione, ma non costituiscono elemento di valutazione della responsabilità dirigenziale
d	costituiscono eventuale causa di responsabilità per danno all'immagine dell'amministrazione, ma non sono valutati ai fini della corresponsione della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei responsabili
e	costituiscono eventuale causa di responsabilità per danno all'immagine dell'amministrazione e sono comunque valutati ai fini della corresponsione della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei responsabili
11	**Quali soggetti possono essere definiti "controinteressati" ai sensi dell'art. 22 della Legge n. 241/1990?**
a	tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza
b	tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un

	interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso
c	tutti i soggetti che abbiano un generico interesse ad accedere al documento
d	tutti i soggetti che abbiano un generico interesse a non fare accedere l'interessato al documento
e	le Pubbliche Amministrazioni
12	**L'art. 23 della Legge n. 241/1990 prevede che il diritto di accesso documentale possa essere esercitato nei confronti…**
a	delle amministrazioni, delle aziende autonome e speciali, degli enti pubblici e dei gestori di pubblici servizi
b	delle amministrazioni e degli enti pubblici
c	dell'amministrazione, anche qualora la sua attività sia diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione
d	delle amministrazioni, delle aziende autonome e speciali e dei gestori di pubblici servizi
e	di tutti i soggetti pubblici e privati
13	**Non è prevista, ai sensi dell'art. 24, comma 1, della Legge 241/1990 l'esclusione del diritto d'accesso:**
a	per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo
b	per i documenti riguardanti l'attività amministrativa del Ministero della Difesa e del Ministero dell'Interno
c	nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano
d	nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione
e	nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psico-attitudinale relativi a terzi
14	**La richiesta di accesso documentale ai sensi della Legge n. 241/1990:**
a	non deve essere motivata e può essere rivolta a qualsiasi amministrazione dello Stato
b	può non essere motivata, ma deve essere rivolta all'amministrazione che ha formato il documento o che lo detiene stabilmente
c	deve essere motivata e deve essere rivolta all'amministrazione che ha formato il documento o che lo detiene stabilmente
	deve essere motivata, ma può essere rivolta a qualsiasi amministrazione dello Stato
e	deve essere motivata, ma può essere rivolta a qualsiasi amministrazione dello Stato
15	**In caso di diniego dell'accesso, espresso o tacito, o di differimento dello stesso, il richiedente può…**
a	presentare ricorso al tribunale amministrativo regionale
b	chiedere il riesame della determinazione al difensore civico, nei confronti degli atti delle amministrazioni comunali, provinciali e regionali, o alla Commissione per l'accesso, nei confronti degli atti delle amministrazioni centrali e periferiche dello Stato

c	presentare ricorso al tribunale civile
d	chiedere il riesame della determinazione al Ministero per la Pubblica Amministrazione
e	presentare ricorso al Consiglio di Stato
16	**L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento dei dati personali che lo riguardano quando…**
a	il trattamento dei dati personali è effettuato con mezzi automatizzati
b	il trattamento si basa sul consenso dell'interessato o risulta necessario per l'esecuzione di un contratto tra l'interessato e il titolare del trattamento
c	il trattamento dei dati personali è effettuato verso paesi terzi o organizzazioni internazionali
d	il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo
e	l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali
17	**Ai sensi del Regolamento UE 2016/679, la certificazione…**
a	esclude che il titolare del trattamento debba fornire all'interessato informazioni relative al trattamento di dati personali che lo riguardano
b	è volontaria e accessibile attraverso una procedura trasparente
c	è rilasciata al titolare del trattamento per un periodo massimo di sei anni
d	è rilasciata al titolare del trattamento per un periodo massimo di dieci anni
e	riduce la responsabilità del titolare del trattamento riguardo alla conformità al Regolamento UE 2016/679
18	**L'interessato del trattamento dei dati personali è…**
a	la persona fisica, identificata o identificabile, a cui si riferiscono i dati personali
b	la persona giuridica, identificata o identificabile, a cui si riferiscono i dati personali
c	la persona giuridica che tratta i dati personali per il perseguimento di un proprio legittimo interesse
d	la persona fisica o giuridica che riceve comunicazione di dati personali
e	la persona fisica o giuridica, identificata o identificabile, a cui si riferiscono i dati personali
19	**Quali figure sono espressamente disciplinate all'interno del Regolamento UE 2016/679?**
a	Il responsabile della protezione dei dati
b	Il responsabile del trattamento
c	Il contitolare del trattamento
d	Il chief privacy officer
e	L'amministratore di sistema
20	**Ai sensi dell'articolo 2-quinquies del decreto legislativo n. 196/2003:**
a	il minore che ha compiuto i 13 anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione
b	il minore che ha compiuto i 14 anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione
c	il minore che ha compiuto i 16 anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione
d	il minore che ha compiuto i 17 anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione
e	è necessario il consenso del titolare della responsabilità genitoriale affinché sia lecito il

	trattamento dei dati personali di un minore in relazione all'offerta diretta di servizi della società dell'informazione
21	**Ai sensi dell'articolo 97 del Regolamento UE 2016/679, la Commissione europea trasmette al Parlamento europeo e al Consiglio europeo relazioni di valutazione e sul riesame del suddetto Regolamento:**
a	entro il 25 maggio 2020 e, successivamente, ogni due anni
b	entro il 25 maggio 2020 e, successivamente, ogni quattro anni
c	entro il 25 maggio 2020 e, successivamente, ogni sei anni
d	entro il 25 maggio 2020 e, successivamente, ogni otto anni
e	entro il 25 maggio 2020 e, successivamente, ogni dieci anni
22	**In caso di violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento non è tenuto a comunicare la violazione all'interessato quando:**
a	il titolare del trattamento ha precedentemente notificato la violazione all'autorità di controllo competente
b	il titolare del trattamento ha precedentemente notificato la violazione all'autorità di controllo competente e al responsabile per la protezione dei dati
c	il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto di violazione
d	il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
e	la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede ad una comunicazione pubblica o a una misura simile
23	**Il Regolamento UE 2016/679 si applica:**
a	al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi
b	al trattamento parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi
c	al trattamento interamente o parzialmente automatizzato di dati personali
d	al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi
e	al trattamento interamente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi
24	**Il Comitato europeo per la protezione dei dati personali è composto:**
a	dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro, o dai rispettivi rappresentanti
b	dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo per la protezione dei dati, o dai rispettivi rappresentanti
c	dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro, dal garante europeo per la protezione dei dati e dai componenti del "Gruppo di lavoro articolo 29 per la protezione dei dati", o dai rispettivi rappresentanti
d	dal garante europeo per la protezione dei dati e dai componenti del "Gruppo di lavoro articolo 29 per la protezione dei dati", o dai rispettivi rappresentanti
e	da un membro del Parlamento europeo, da un membro della Commissione europea, da un

	membro del Consiglio europeo e dal garante europeo per la protezione dei dati
25	**L'interessato può esercitare il diritto alla portabilità dei dati qualora…**
a	il trattamento sia effettuato con mezzi automatizzati
b	il trattamento risulti necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica
c	il trattamento dei dati personali risulti necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento
d	il trattamento risulti necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Inoltre, qualora il trattamento sia effettuato con mezzi automatizzati
e	l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Inoltre, qualora il trattamento sia effettuato con mezzi automatizzati
26	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, l'acronimo ABSC indica:**
a	Agid Basic Security Control
b	Agid Broadband System Control
c	Activity Business System Center
d	Activity Board Security Center
e	Automatic Broadband System Control
27	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per l'USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE:**
a	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
b	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
c	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
d	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
e	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.
28	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per l'USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE:**
a	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.
b	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.
c	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
d	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.
e	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli

	amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.
29	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per le DIFESE CONTRO I MALWARE:**
a	Installare su tutti i dispositivi firewall ed IPS personali.
b	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali
c	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file
d	Installare sistemi di analisi avanzata del software sospetto.
e	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.
30	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per le DIFESE CONTRO I MALWARE:**
a	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.
b	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.
c	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.
d	Installare sistemi di analisi avanzata del software sospetto.
e	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.
31	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per effettuare COPIE DI SICUREZZA:**
a	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
b	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
c	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.
d	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.
e	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.
32	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per effettuare COPIE DI SICUREZZA:**
	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.
b	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.
c	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.
d	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.
e	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.

33	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per la PROTEZIONE DEI DATI:**
a	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
b	Bloccare il traffico da e verso url presenti in una blacklist.
c	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.
d	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.
e	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.
34	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per la PROTEZIONE DEI DATI:**
a	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro
b	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti
c	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line
d	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository
e	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto
35	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D.:**
a	ha la responsabilità della attuazione delle misure minime di sicurezza informatica
b	può designare un dirigente per l'attuazione delle misure minime di sicurezza informatica
c	non è implicato nel processo di definizione e attuazione delle misure minime di sicurezza informatica
d	non può designare alcuno per l'attuazione delle misure minime di sicurezza informatica
e	può designare qualsiasi impiegato dell'amministrazione, purché adeguatamente formato per l'attuazione delle misure minime di sicurezza informatica
36	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, il modulo di implementazione delle misure di sicurezza:**
a	dovrà essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura
b	dopo la sottoscrizione deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso
c	può essere firmato analogicamente
d	può essere firmato analogicamente purchè approvato dal consiglio di Amministrazione
e	deve essere firmato analogicamente

37	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per effettuare l'INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI:**
a	Implementare un inventario delle risorse attive
b	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete
c	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete, registrando almeno l'indirizzo IP
d	Utilizzareicertificatilatoclientpervalidareeautenticareisistemiprimadellaconnessione a una rete locale
e	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete
38	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per effettuare l'INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI:**
a	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie
b	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati a prescindere che siano collegati o meno alla rete dell'organizzazione
c	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. Il 802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati
d	Utilizzareicertificatilatoclientpervalidareeautenticareisistemiprimadellaconnessione a una rete locale
e	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate
39	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per effettuare l'INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI:**
a	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco
b	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato
c	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch
d	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate
e	Utilizzare macchine virtuali e/o sistemi air-gapped1 per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete

40	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per effettuare l'INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI:**
a	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch
b	Utilizzare macchine virtuali e/o sistemi air-gapped1 per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete
c	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
d	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati
e	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie
41	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER:**
a	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi
b	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione
c	Le immagini d'installazione devono essere memorizzate offline
d	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standar.
e	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri)
42	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER:**
a	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco
b	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate
c	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard
d	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza
e	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità

43	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello minimo per la VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ:**
a	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche
b	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza
c	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
d	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio
e	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato
44	**Secondo la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, quali sono ritenute misure ABSC di livello alto per la VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ:**
a	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project)
b	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato
c	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP
d	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza
e	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione
45	**La CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, introduce come misura ABSC di livello medio e alto per la VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ la possibilità di eseguire le scansioni di vulnerabilità in modalità privilegiata sia localmente che in remoto. Per effettuare queste scansioni quali dei seguenti strumenti si usano:**
a	Firewall
b	IDS
c	IPS
d	Antivirus
e	Anti-malware
46	**La CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, introduce come misura ABSC di livello alto per l'USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE sistemi di autenticazione a più fattori. Quali delle seguenti tecnologie può essere utilizzata per la realizzazione dell'autenticazione a più fattori:**
a	smart card

b	certificati digitali
c	one time password (OTP)
d	token
e	biometria e sistemi analoghi
47	**La CIRCOLARE AGID del 18 aprile 2017, n. 2/2017 definisce:**
a	le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi
b	i livelli minimi di sicurezza che devono garantire i sistemi informativi
c	tutte le misure per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi
d	le procedure organizzative e tecniche che devono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi
e	le procedure organizzative che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi
48	**Le amministrazioni destinatarie della CIRCOLARE AGID del 18 aprile 2017, n. 2/2017 sono:**
a	le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165
b	le società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione
c	le Università
d	i soggetti di cui all'art. 2, comma 2 del C.A.D.
e	le società a prevalenza di capitale privato
49	**La CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, introduce come misura ABSC di livello alto per effettuare l'INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI l'uso del protocollo 802.1x. L'utilizzo di questo protocollo permette:**
a	controllare quali dispositivi possono essere connessi alla rete
b	limitare i dispositivi che possono essere connessi alla rete
c	limitare e controllare quali dispositivi possono essere connessi alla rete
d	bloccare tutti i dispositivi che rappresentano una minaccia alla sicurezza
e	inventariare in modo automatico tutti i dispositivi connessi alla rete
50	**La CIRCOLARE AGID del 18 aprile 2017, n. 2/2017, introduce come misura ABSC di livello medio e alto per PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER l'hardening del sistema. L'hardening comprende tipicamente:**
a	l'eliminazione degli account non necessari
b	la disattivazione o eliminazione dei servizi non necessari
c	la configurazione di stack e heaps non eseguibili
d	l'applicazione di patch
e	la chiusura di porte di rete aperte e non utilizzate