International Federation of Biosafety Associations

Certificação Profissional em Ciberbioproteção

Conteúdo do Exame, Questões de Amostra e Referências

A Certificação Profissional (PC) da IFBA em Ciberbioproteção identifica indivíduos com competências demonstradas na mitigação de riscos de segurança cibernética em laboratórios biológicos. Isso inclui riscos de Tecnologia da Informação (TI) e Tecnologia Operacional (TO), a fim de proteger pesquisas biológicas sensíveis, dados, bases de dados, e instalações e equipamentos laboratoriais contra acesso ilícito ou não autorizado, roubo, adulteração ou outras formas de uso indevido.

A PC em Ciberbioproteção é adequada para uma ampla gama de profissionais que trabalham diretamente ou no entorno de laboratórios biológicos e de biotecnologia, laboratórios farmacêuticos e de pesquisa, profissionais tais como assessores de gestão de biorrisco, oficiais de biossegurança, pessoal científico de laboratório, tecnólogos biomédicos, profissionais de TI e de segurança cibernética, pessoal de operações e manutenção de instalações, pessoal de segurança, gestão e administração.

Para fins desta certificação, Ciberbioproteção é definida como “a proteção e mitigação contra uso indevido, exploração, dano ou interrupção de informações, dados, bases de dados, equipamentos e instalações valiosos na interface entre laboratórios e instalações relacionadas às ciências da vida e os ambientes digitais.”

O Corpo de Conhecimento (BOK) apresentado abaixo identifica 5 domínios (áreas temáticas) e 45 declarações de conhecimento e tarefas que definem a competência para certificação em Ciberbioproteção. O conteúdo do exame é baseado neste BOK, e cada questão do exame está vinculada a uma das declarações abaixo.

Domínio A – Conceitos de Ciberbioproteção

1. Descrever o campo emergente da ciberbioproteção na interface entre segurança cibernética, segurança cibernética física, gestão da qualidade, biossegurança e bioproteção.
2. Descrever as ameaças e vulnerabilidades associadas à ciberbioproteção em setores distintos das ciências da vida, ciências biomédicas, biotecnologia, biologia sintética e outros setores da bioeconomia.

3. Identificar maneiras pelas quais as vulnerabilidades de ciberbioproteção em laboratórios biológicos apresentam risco à integridade de materiais biológicos e dados digitais associados a eles, aos trabalhadores de laboratório, à comunidade pública envolvida, aos animais e ao meio ambiente.
4. Compreender como dispositivos e equipamentos de rede aumentam as vulnerabilidades e os riscos de ciberbioproteção e como reduzir esses riscos (por exemplo, segregar dispositivos menos seguros da rede, remover dispositivos, não críticos ou não seguros, de ambientes conectados a ambientes de Internet das Coisas).
5. Saber como identificar, avaliar, reduzir e responder a ameaças, riscos e incidentes envolvendo ciberbioproteção em laboratórios biológicos em associação aos seus ativos com componentes digitais, equipamentos em rede, dispositivos e sistemas da instalação.
6. Compreender os papéis e responsabilidades do pessoal responsável pela ciberbioproteção (por exemplo, oficiais de biossegurança, cientistas de laboratório, pessoal de manutenção, pessoal de TI, administração, segurança) além de compreender a importância da comunicação regular entre os responsáveis pela ciberbioproteção.
7. Saber como desenvolver e implementar programas de treinamento em ciberbioproteção, promover conscientização em ciberbioproteção e boas práticas pessoais de segurança cibernética no ambiente de trabalho laboratorial.
8. Estar familiarizado e compreender como desenvolver/atualizar políticas organizacionais e Procedimentos Operacionais Padrão (POPs) em alinhamento com as melhores práticas relevantes de ciberbioproteção.

Domínio B – Fundamentos de Segurança Cibernética

9. Compreender as opções disponíveis para quando um adversário mal-intencionado conduzir vigilância física e cibernética de uma instalação para objetivos maldosos que podem ser sutis, indiretos ou inesperados, e como reduzir esses riscos potenciais.
10. Compreender táticas e técnicas de intrusão que podem ser usadas por um adversário mal-intencionado para obter acesso e explorar dados e sistemas (por exemplo, engenharia social, explorações de dia zero, compromissos na cadeia de suprimentos de software, redes, armazenamento em nuvem, usuários, e-mail, aplicações web, portais de acesso remoto, dispositivos móveis).
11. Definir os termos: Tecnologia da Informação (TI), Tecnologia Operacional (TO) e Internet das Coisas (IoT).
12. Descrever as 3 categorias comuns de autenticação multifatorial, ou seja, conhecimento, posse, inerência.
13. Compreender os princípios de controle de acesso (por exemplo, privacidade por design, proteção de dados por design, política de uso aceitável, contas de usuário com privilégios mínimos, configuração de contas de usuário e permissões de segurança em múltiplos ambientes, gestão de direitos digitais).

14. Compreender os princípios de gestão de identidade e acesso (por exemplo, gestão de permissões de entidades e grupos, configuração de unidades organizacionais e objetos).
15. Compreender os princípios de proteção física (por exemplo, estabelecimento de controle físico de acesso) e proteção de mídias (por exemplo, sanitização ou destruição adequada de mídias).
16. Compreender os princípios de proteção de sistemas e comunicações (por exemplo, monitoramento de dispositivos de fronteira externos e internos, implementação de sub-redes).
17. Compreender os princípios de integridade de sistemas e informações (por exemplo, identificação de problemas do sistema, implantação de assinaturas baseadas em rede/host, realização de varreduras antivírus periódicas).

Domínio C – Riscos de Tecnologia da Informação (TI) em Laboratórios Biológicos

18. Descrever os diferentes tipos de dados armazenados e transmitidos por meio de plataformas e equipamentos de tecnologia da informação no laboratório biológico que podem apresentar um fluxo de dados de interesse para adversários.
19. Compreender como vulnerabilidades de dados afetam negativamente a gestão da qualidade por meio de perda de confidencialidade (isto é, perda de dados), perda de disponibilidade (isto é, interrupção operacional) e perda de integridade (isto é, dados alterados).
20. Descrever como a exfiltração de dados pode ocorrer tanto por um adversário mal-intencionado interno quanto externo e como tecnologias de criptografia de bases de dados podem ser usadas para proteger informações em bases de dados biológicas.
21. Descrever as formas pelas quais equipamentos de laboratório em rede podem ser explorados remotamente/digitalmente para comprometer a integridade da pesquisa, alterar sequências genômicas, manipular características de agentes biológicos e criar produtos biológicos nocivos.
22. Descrever como o uso de Zonas Desmilitarizadas e Zonas de Confiança pode ser usado para aumentar a segurança de equipamentos laboratoriais em rede e infraestrutura.
23. Descrever como algoritmos criptográficos podem ser usados para senhas, autenticação multifatorial, Rede Privada Virtual, e criptografia de dados em repouso e em trânsito podem ser incorporados na política de ciberbioproteção de um laboratório.
24. Compreender a importância de avaliações periódicas de vulnerabilidade e testes de penetração de rede/aplicação delimitados que podem ser usados para identificar e mitigar vulnerabilidades.
25. Saber como reduzir vulnerabilidades de ciberbioproteção apresentadas pelo uso de dispositivos pessoais (por exemplo, laptops pessoais e celulares) para acessar sistemas relacionados ao laboratório.
26. Compreender as vulnerabilidades associadas ao uso de tecnologias de espectro sem fio e equipamentos conectados à internet, e como dispositivos sem fio podem aumentar sua superfície de ataque e possibilitar novos vetores de ataque para adversários.

27. Descrever quais vulnerabilidades e informações sensíveis podem ser reveladas a adversários por meio de documentos de controle administrativo (por exemplo, procedimentos de resposta a emergências, planos de programas de segurança), documentos de orçamento e planejamento, documentos contratuais, plantas e esquemas de laboratórios, salas de apoio e espaços mecânicos.
28. Descrever maneiras de restringir a divulgação de informações sensíveis e vulnerabilidades de instalações para contratados externos de manutenção de instalações, prestadores de serviços de equipamentos e fornecedores.
29. Compreender as vulnerabilidades de segurança cibernética associadas a sistemas de inventário de patógenos em rede e Sistemas de Gerenciamento de Informações de Laboratório.
30. Saber como identificar e mitigar vulnerabilidades de atividades relacionadas ao laboratório realizadas por pessoal que podem resultar na divulgação de informações sensíveis (por exemplo, compartilhamento legítimo de dados para pesquisa, ensino ou fins comerciais).

Domínio D – Riscos de Tecnologia Operacional (OT) em Laboratórios Biológicos

31. Compreender como a inovação tecnológica em “laboratórios inteligentes” (ou seja, laboratórios com dispositivos conectados capazes de monitoramento e controle remoto, chaves inteligentes) está sujeita a vulnerabilidades de segurança cibernética.
32. Compreender as vulnerabilidades de segurança cibernética com o uso de cadernos eletrônicos de laboratório e assistentes pessoais virtuais acionados por voz que utilizam comandos de voz no laboratório.
33. Saber como sistemas de automação predial em rede e softwares de gerenciamento de energia estão sujeitos a vulnerabilidades de segurança cibernética.
34. Descrever as maneiras pelas quais um sistema de controle de acesso físico de um laboratório poderia ser explorado remotamente/digitalmente para comprometer a segurança.
35. Descrever as maneiras pelas quais o sistema de automação predial de um laboratório de biocontenção poderia ser explorado remotamente/digitalmente para comprometer a biossegurança, a contenção, a segurança da vida e a integridade de materiais/dados biológicos.
36. Descrever as maneiras pelas quais sistemas e equipamentos de descontaminação de um laboratório biológico poderiam ser explorados remotamente/digitalmente para comprometer a biossegurança e a biocontenção.
37. Descrever as maneiras pelas quais salas de alojamento de animais e sistemas de gaiolas de contenção poderiam ser explorados remotamente/digitalmente e os impactos potenciais de tal intrusão.
38. Compreender os riscos potenciais de segurança cibernética que podem comprometer a cadeia de suprimentos de um laboratório e como esses riscos podem ser minimizados e revertidos se detectados.

Domínio E – Preparação & Resposta a Incidentes de Ciberbioproteção

39. Saber como realizar um passo a passo guiado (walkthrough) completo da instalação com o propósito de desenvolver um plano de mitigação de ameaças de ciberbioproteção e resposta a incidentes.
40. Descrever o desenvolvimento de um plano abrangente de mitigação de ameaças de ciberbioproteção, resposta a incidentes e comunicação para minimizar danos, conter a ameaça e manter a biossegurança e a bioproteção.
41. Compreender os papéis e responsabilidades de pessoal chave na resposta a incidentes de ciberbioproteção tanto dentro da organização quanto de especialistas externos.
42. Saber antecipadamente onde obter assistência externa adicional confiável e verificada para identificar, responder e recuperar de incidentes de ciberbioproteção.
43. Saber quando e como envolver agências de aplicação da lei que possam ser necessárias para responder, investigar, coletar evidências probatórias e conduzir entrevistas.
44. Conhecer os canais de comunicação, como relatar e a quem relatar incidentes potenciais e detectados de ciberbioproteção.
45. Saber como conduzir exercícios regulares da equipe de resposta a incidentes de ciberbioproteção, incluindo exercícios de mesa.

Plano do Exame (*Exam Blueprint*)

O seguinte representa o número de questões em cada domínio que estão incluídas no exame:

Plano do Exame Certificação Profissional em Ciberbioproteção Nota de corte – 70%	
Domínio	**Número de Questões**
A) Conceitos de Ciberbioproteção	19
B) Fundamentos de Segurança Cibernética	18
C) Riscos de Tecnologia da Informação (TI) em Laboratórios Biológicos	28
D) Riscos de Tecnologia Operacional (OT) em Laboratórios Biológicos	12
E) Preparação & Resposta a Incidentes de Ciberbioproteção	13

Questões de Amostra (*Sample Questions*)

De forma que os candidatos possam estar familiarizados com a natureza e forma das questões do exame, as seguintes questões são fornecidas como exemplos. Um asterisco marca a resposta correta.

1. Qual cenário MELHOR representa uma preocupação relacionada à ciberbioproteção no ambiente laboratorial biológico atual?

    a) Laboratórios com pouca segurança podem resultar em indivíduos não autorizados ganhando acesso e roubando patógenos dos freezers do laboratório.
    b) Equipamentos laboratoriais e dispositivos IoT conectados à internet podem ser hackeados para acessar e alterar dados laboratoriais confidenciais.*
    c) Pesquisadores de laboratório podem vender informações científicas proprietárias e dados para uma organização de pesquisa concorrente.
    d) Resíduos podem ser inadequadamente descontaminados antes de sair do laboratório para descarte externo.

2. Complete a frase: Usar um(a)_____ para verificar a identidade de um usuário da rede é um exemplo de autenticação multifatorial para diminuir a probabilidade de um ataque cibernético.
    a) senha e nome de usuário
    b) pergunta de segurança e código PIN
    c) código único de 4 dígitos enviado via SMS*
    d) escaneamento de impressão digital e reconhecimento facial

3. O departamento de TI está desenvolvendo uma política e procedimentos sobre funcionários trazerem seus próprios dispositivos pessoais" (*Bringing Their Own Personal Devices* - BYOD) para o laboratório. Qual afirmação é VERDADEIRA?

    a) Uma política BYOD no laboratório é aceitável, e nenhum procedimento específico é necessário se os dispositivos não forem usados para acessar informações e dados laboratoriais sensíveis.
    b) A política deve proibir BYOD devido aos desafios exclusivos de segurança cibernética e ao maior nível de risco em todos os ambientes laboratoriais que manipulam agentes biológicos.
    c) Os procedimentos de segurança cibernética já implementados para proteger dispositivos e dados laboratoriais geralmente são adequados para fornecer segurança eficaz também para BYOD.
    d) Políticas e procedimentos específicos precisam ser implementados para abordar os riscos de TI exclusivos do BYOD para a organização e os riscos de privacidade para os funcionários.*

4. Infraestruturas de laboratório de contenção biológica podem ser projetadas com equipamentos e sistemas vulneráveis a ataques cibernéticos. Complete a frase: Ao considerar segurança cibernética e sistemas de contenção predial, gestores de instalações devem _____ .

    a) comunicar-se regularmente com seu departamento de TI e fornecedores para implementar soluções de segurança cibernética para infraestrutura existente, contratos de serviço e manutenção, e novas instalações*
    b) confiar em seu departamento de TI, que possui expertise e responsabilidade para desenvolver e adotar políticas e procedimentos de segurança cibernética para infraestrutura e sistemas prediais do laboratório
    c) confiar em fornecedores que são responsáveis por garantir que seus sistemas prediais, equipamentos e pessoal de serviço estejam seguros contra vulnerabilidades e cumprindo melhores práticas de segurança cibernética
    d) colaborar com gestores de laboratório para realizar um escaneamento de vulnerabilidade cibernética e teste de penetração dos sistemas de contenção predial pelo menos uma vez por mês

5. Complete a frase: Ao desenvolver um plano de resposta a incidentes de segurança cibernética para seu laboratório biológico, uma organização deve _____ .

    a) preparar e desenvolver instruções passo a passo para todos os funcionários lidarem com todos os incidentes potenciais que possam impactar negativamente a organização
    b) focar em estar geralmente preparada em toda a organização, com maior ênfase em como lidar com incidentes que utilizam vetores de ataque comuns*
    c) limitar estritamente o compartilhamento de informações sobre todos os aspectos do plano dentro da organização para reduzir a probabilidade de ataques cibernéticos de ameaças internas
    d) estabelecer procedimentos escritos para lidar com múltiplos incidentes por ordem de chegada para economizar tempo dos responsáveis por incidentes

Referências

Além do conhecimento da terminologia e fundamentos básicos de segurança cibernética, alguma preparação sugerida para o exame pode incluir, mas não se limitar aos seguintes recursos:

Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience, Daniel S. Schabacker et al, Frontiers in Bioengineering and Biotechnology, 29 March 2019.

Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape, Lauren C. Richardson et al, Frontiers in Bioengineering and Biotechnology, 06 June 2019.

Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy, Randall S. Murch et al, Frontiers in Bioengineering and Biotechnology, 05 April 2018.

Cyberbiosecurity Implications for the Laboratory of the Future, J. Craig Reed & Nicolas Dunaway, Frontiers in Bioengineering and Biotechnology, 21 August 2019.

Cyberbiosecurity: From Naïve Trust to Risk Awareness, Jean Peccoud et al, Trends in Biotechnology, January, 2018.

Cybersecurity Incident Response Exercise Guidance, Larry G. Wlosinski et al, ISACA Journal, Vol 1, January 2022.

Information technology - Security techniques - Guidelines for Cybersecurity, International Standards Organization. ISO/IEC 27032:2012.

Facing the 202 Pandemic: What does Cyberbiosecurity Want us to Know to Safeguard the future? Siguna Meuller, Biosafety & Health, February, 2021.

Computer Security Incident Handling Guide, US National Institute of Standards & Technology NIST, 2012.

Cyberthreats to Biotechnology, US Dept. Health & Human Services, 2021.

Guidelines for Media Sanitation, US National Institute of Standards & Technology, 2014.

Framework for Improving Critical Infrastructure Cybersecurity, US National Institute of Standards & Technology, 2018.

Mobile Device Best Practices, US National Security Agency, 2020.

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, US National Institute of Standards & Technology, 2019.