



## **Certificación Profesional en Ciberbiocustodia** *Contenido del examen, preguntas de muestra & referencias*

La Certificación Profesional (CP) en Ciberbiocustodia de la Federación Internacional de Asociaciones de Bioseguridad (*IFBA, por sus siglas en inglés*) identifica a individuos con competencias demostradas en la mitigación de riesgos de ciberseguridad en laboratorios biológicos. Esto incluye riesgos relacionados con Tecnología de la Información (TI) y Tecnología Operativa (TO) con el fin de proteger investigaciones biológicas sensibles, datos, bases de datos, así como instalaciones y equipos de laboratorio, contra accesos ilícitos o no autorizados, robo, manipulación u otras formas de uso indebido.

La CP en Ciberbiocustodia es adecuada para una amplia gama de profesionales que trabajan en y alrededor de laboratorios biológicos, laboratorios de biotecnología, farmacéuticos y de investigación, tales como asesores en gestión de riesgos biológicos, oficiales de bioseguridad, personal científico de laboratorio, tecnólogos biomédicos, personal de TI y ciberseguridad, personal de operaciones y mantenimiento de instalaciones, personal de seguridad, gerencia y administración.

Para los fines de esta certificación, la Ciberbiocustodia se define como: “la protección y mitigación del uso indebido, explotación, daño o interrupción de información valiosa, datos, bases de datos, equipos e instalaciones en la interfaz entre el laboratorio biológico, las instalaciones relacionadas con las ciencias de la vida y los entornos digitales.”

El Cuerpo de Conocimiento (*Body of Knowledge, BOK*) que se presenta a continuación identifica 5 dominios (áreas temáticas) y 45 declaraciones de conocimientos/tareas que definen la competencia para la certificación en Ciberbiocustodia. El contenido del examen se basa en este *BOK* y cada pregunta del examen está vinculada a una de las declaraciones indicadas a continuación.

### **Dominio A – Conceptos de Ciberbiocustodia**

1. Describir el campo emergente de la ciberbiocustodia en la interfaz entre la ciberseguridad, la seguridad ciberfísica, la gestión de la calidad, la bioseguridad y la biocustodia.
2. Describir las amenazas y vulnerabilidades asociadas a la ciberbiocustodia en múltiples sectores distintos de las ciencias de la vida, ciencias biomédicas, biotecnología, biología sintética y otros ámbitos de la bioeconomía.

3. Identificar de qué manera las vulnerabilidades en ciberbiocustodia en los laboratorios biológicos representan un riesgo para la integridad de los materiales biológicos y los datos digitales asociados, el personal del laboratorio, la comunidad pública circundante, los animales y el medio ambiente.
4. Comprender cómo los dispositivos y equipos conectados en red aumentan las vulnerabilidades y los riesgos de ciberbiocustodia, y cómo reducir dichos riesgos (p. ej., separando dispositivos menos seguros de la red, eliminando dispositivos del Internet de las Cosas [*IoT, por sus siglas en inglés*] que no sean críticos o seguros).
5. Saber cómo identificar, evaluar, reducir y responder ante amenazas, riesgos e incidentes de ciberbiocustodia en laboratorios biológicos asociados con sus activos que poseen componentes digitales, equipos conectados en red, dispositivos y sistemas de las instalaciones.
6. Comprender los roles y responsabilidades del personal clave en ciberbiocustodia (p. ej., oficiales de bioseguridad, científicos de laboratorio, personal de mantenimiento de instalaciones, personal de TI, administración, seguridad) y la importancia de una comunicación regular entre ellos.
7. Saber cómo desarrollar e implementar programas de capacitación en ciberbiocustodia, fomentar la concientización en la materia y promover buenas prácticas personales de ciberseguridad en el entorno laboral del laboratorio.
8. Estar familiarizado con el desarrollo y/o actualización de políticas organizacionales y Procedimientos Estandarizados de Operación alineados con las mejores prácticas relevantes en ciberbiocustodia.

## **Dominio B – Fundamentos de la Ciberseguridad**

9. Comprender las opciones disponibles para un adversario a fin de llevar a cabo vigilancia física y cibernética de una instalación con objetivos que pueden ser sutiles, indirectos o inesperados, así como cómo reducir estos riesgos potenciales.
10. Comprender las tácticas y técnicas de intrusión que pueden ser utilizadas por un adversario para acceder y explotar datos y sistemas (p. ej., ingeniería social, vulnerabilidades de día cero, compromisos en la cadena de suministro de software, redes, almacenamiento en la nube, usuarios, correo electrónico, aplicaciones web, portales de acceso remoto, dispositivos móviles).
11. Definir los términos: Tecnología de la Información (*TI*), Tecnología Operativa (*TO*) e Internet de las Cosas (*IoT, por sus siglas en inglés*).
12. Describir las tres categorías comunes de autenticación multifactor (es decir, conocimiento, posesión, inherencia).
13. Comprender los principios del control de acceso (p. ej., privacidad desde el diseño, protección de datos desde el diseño, política de uso aceptable, cuentas de usuario con privilegios mínimos, configuración de cuentas de usuario y permisos de seguridad en múltiples entornos, gestión de derechos digitales).

14. Comprender los principios de la gestión de identidades y accesos (p. ej., gestión de permisos para entidades y grupos, configuración de unidades organizacionales y objetos).
15. Comprender los principios de la protección física (p. ej., establecer controles de acceso físico) y de la protección de medios (p. ej., sanitización o destrucción adecuada de medios).
16. Comprender los principios de protección de sistemas y comunicaciones (p. ej., monitoreo de dispositivos de frontera externa e interna, implementación de subredes).
17. Comprender los principios de integridad del sistema y la información (p. ej., identificación de fallas del sistema, implementación de firmas basadas en red y host, realización periódica de análisis antivirus).

## **Dominio C – Riesgos en Tecnología de la Información (TI) en Laboratorios Biológicos**

18. Describir los diferentes tipos de datos almacenados y transmitidos a través de plataformas y equipos de tecnología de la información en el laboratorio biológico que podrían representar un flujo de datos de interés para posibles adversarios.
19. Comprender cómo las vulnerabilidades en los datos afectan negativamente a la gestión de la calidad mediante la pérdida de confidencialidad (es decir, pérdida de datos), pérdida de disponibilidad (es decir, interrupción operativa) y pérdida de integridad (es decir, alteración de los datos).
20. Describir cómo puede producirse la exfiltración de datos tanto por parte de un adversario interno como externo, y cómo las tecnologías de cifrado de bases de datos pueden utilizarse para proteger la información contenida en bases de datos biológicas.
21. Describir las formas en que el equipo de laboratorio conectado en red puede ser explotado digitalmente o de forma remota para comprometer la integridad de la investigación, alterar secuencias genómicas, manipular las características de agentes biológicos y generar productos biológicos dañinos.
22. Describir cómo el uso de Zonas Desmilitarizadas (*DMZ*) y Zonas de Confianza (*Trust Zones*) puede mejorar la seguridad de los equipos de laboratorio conectados en red y de la infraestructura.
23. Describir cómo los algoritmos criptográficos pueden utilizarse para la gestión de contraseñas, autenticación multifactor, uso de redes privadas virtuales (*VPN*) y el cifrado de datos en reposo y en tránsito, como parte de una política de ciberbiocustodia en el laboratorio.
24. Comprender la importancia de realizar evaluaciones periódicas de vulnerabilidades y pruebas de penetración de red o aplicaciones con un alcance definido, como herramientas para identificar y mitigar vulnerabilidades.
25. Saber cómo reducir las vulnerabilidades en ciberbiocustodia derivadas del uso de dispositivos personales (p. ej., computadoras portátiles y teléfonos celulares personales) para acceder a sistemas relacionados con el laboratorio.

26. Comprender las vulnerabilidades asociadas con el uso de tecnologías de espectro inalámbrico y equipos conectados a internet, y cómo estos dispositivos pueden aumentar la superficie de ataque y habilitar nuevos vectores de ataque para los adversarios.
27. Describir qué vulnerabilidades e información sensible pueden ser reveladas a adversarios a través de documentos administrativos de control (p. ej., procedimientos de respuesta ante emergencias, planes de programas de seguridad y protección), documentos presupuestarios y de planificación, contratos, planos y esquemas de laboratorios, salas auxiliares y espacios mecánicos.
28. Describir formas de restringir la divulgación de información sensible y vulnerabilidades de las instalaciones a contratistas externos de mantenimiento, proveedores de servicios técnicos y proveedores de equipos.
29. Comprender las vulnerabilidades de ciberseguridad asociadas a los sistemas en red de inventario de patógenos y a los Sistemas de Gestión de Información de Laboratorio (*LIMS, por sus siglas en inglés*).
30. Saber cómo identificar y mitigar vulnerabilidades en actividades relacionadas con el laboratorio realizadas por personal que podrían resultar en la divulgación de información sensible (p. ej., intercambio legítimo de datos para fines de investigación, enseñanza o comerciales).

### **Dominio D – Riesgos en Tecnología Operativa (TO) en Laboratorios Biológicos**

31. Comprender cómo la innovación tecnológica en “laboratorios inteligentes” (es decir, laboratorios con dispositivos conectados en red capaces de monitoreo y control remoto, llaves inteligentes) está sujeta a vulnerabilidades de ciberseguridad.
32. Comprender las vulnerabilidades de ciberseguridad asociadas al uso de cuadernos electrónicos de laboratorio y asistentes virtuales personales activados por comandos de voz en el entorno del laboratorio.
33. Conocer cómo los sistemas de automatización de edificios conectados en red y el software de gestión energética están expuestos a vulnerabilidades de ciberseguridad.
34. Describir las formas en que los sistemas de control de acceso físico de un laboratorio podrían ser explotados de manera remota o digital para comprometer la seguridad.
35. Describir las formas en que los sistemas de automatización de edificios en laboratorios de biocontención podrían ser explotados de manera remota o digital para comprometer la bioseguridad, la contención, la seguridad vital y la integridad de los materiales y datos biológicos.
36. Describir las formas en que los sistemas y equipos de descontaminación de un laboratorio biológico podrían ser explotados de manera remota o digital para comprometer la bioseguridad y la biocontención.
37. Describir las formas en que las salas de alojamiento de animales y los sistemas de contención en jaulas podrían ser explotados de forma remota o digital, y los posibles impactos de dicha intrusión.

38. Comprender los riesgos potenciales de ciberseguridad que pueden comprometer la cadena de suministro de un laboratorio y cómo dichos riesgos pueden minimizarse y revertirse si se detectan.

### **Dominio E – Preparación y Respuesta ante Incidentes de Ciberbiocustodia**

39. Saber cómo realizar un recorrido completo por las instalaciones con el fin de desarrollar un plan de mitigación de amenazas e incidentes de ciberbiocustodia.
40. Describir el desarrollo de un plan integral de mitigación de amenazas, respuesta ante incidentes y comunicación en ciberbiocustodia, con el objetivo de minimizar daños, contener la amenaza y mantener la bioseguridad y la biocustodia.
41. Comprender los roles y responsabilidades del personal clave para la respuesta ante incidentes de ciberbiocustodia, tanto dentro de la organización como de especialistas externos.
42. Saber de antemano dónde obtener asistencia adicional externa confiable y validada para la identificación, respuesta y recuperación ante incidentes de ciberbiocustodia.
43. Saber cuándo y cómo involucrar a las agencias de aplicación de la ley (*agencias gubernamentales*) que podrían ser requeridas para responder, investigar, recolectar evidencia probatoria y realizar entrevistas.
44. Conocer los canales de comunicación, cómo y a quién reportar incidentes de ciberbiocustodia potenciales o detectados.
45. Saber cómo llevar a cabo ejercicios regulares del equipo de respuesta ante incidentes de ciberbiocustodia, incluyendo ejercicios de mesa (*table-top exercises*).

### *Contenido del Examen*

A continuación, se detalla el número de preguntas en cada dominio que están incluidas en el examen:

| <b>Contenido del Examen</b>  |                            |
|--|----------------------------|
| <b>Certificación Profesional en Ciberbiocustodia</b>                       |                            |
| <b>Calificación aprobatoria – 70%</b>                                      |                            |
| <b>Dominio</b>   | <b>Numero de preguntas</b> |
| A) Conceptos de Ciberbiocustodia   | 19                         |
| B) Fundamentos de Ciberseguridad   | 18                         |
| C) Riesgos en Tecnología de la Información (TI) en Laboratorios Biológicos | 28                         |
| D) Riesgos en Tecnología Operativa (TO) en Laboratorios Biológicos         | 12                         |
| E) Preparación y Respuesta ante Incidentes de Ciberbiocustodia             | 13                         |

### *Preguntas Muestra de la Evaluación*

Con el objetivo de familiarizar a los candidatos con la naturaleza y el formato de las preguntas del examen, se presentan los siguientes ejemplos. Un asterisco indica la respuesta correcta.

1. ¿Cuál de los siguientes escenarios representa MEJOR una preocupación relacionada con la ciberbiocustodia en el entorno actual de los laboratorios que manejan agentes biológicos?
  - A. Laboratorios mal asegurados podrían permitir que personas no autorizadas accedan y roben patógenos de los congeladores del laboratorio.
  - B. El equipo de laboratorio y los dispositivos IoT conectados a internet podrían ser hackeados para acceder y alterar datos confidenciales del laboratorio.\*
  - C. Investigadores de laboratorio podrían vender información científica y datos confidenciales a una organización de investigación competidora.
  - D. Los residuos podrían no ser descontaminados adecuadamente antes de salir del laboratorio para su eliminación fuera del sitio.
  
2. Complete el siguiente enunciado: Usar \_\_\_\_\_ para verificar la identidad de un usuario en la red es un ejemplo de autenticación multifactor que disminuye la probabilidad de un ciberataque.
  - A. contraseña y nombre de usuario
  - B. pregunta de seguridad y código PIN
  - C. código de 4 dígitos enviado por SMS una sola vez\*
  - D. escaneo de huella digital y reconocimiento facial
  
3. El departamento de TI está desarrollando una política y procedimientos sobre el ingreso de dispositivos personales (*BYOD, por sus siglas en inglés*) por parte de los empleados al laboratorio. ¿Cuál de los siguientes enunciados es VERDADERO?
  - A. Una política *BYOD* en el laboratorio es aceptable y no se requieren procedimientos específicos si los dispositivos no se utilizan para acceder a información y datos sensibles del laboratorio.
  - B. La política debe prohibir el uso de *BYOD* debido a los desafíos únicos de ciberseguridad y al mayor nivel de riesgo en todos los entornos de laboratorio que manejan agentes biológicos.
  - C. Los procedimientos de ciberseguridad ya implementados para proteger los dispositivos y datos del laboratorio generalmente son adecuados para proporcionar seguridad efectiva al *BYOD* también.
  - D. Se deben implementar políticas y procedimientos específicos que aborden los riesgos únicos del *BYOD* para la TI de la organización y los riesgos de privacidad para los empleados.\*

4. La infraestructura de un laboratorio de biocontención puede estar diseñada con equipos y sistemas vulnerables a ciberataques. Complete la siguiente afirmación: Al considerar la ciberseguridad y los sistemas de contención de edificios, los responsables de las instalaciones deben \_\_\_\_\_.
- A. comunicarse regularmente con su departamento de TI y con los proveedores para implementar soluciones de ciberseguridad en la infraestructura existente, los contratos de servicio y mantenimiento, y las nuevas instalaciones\*
  - B. confiar en su departamento de TI, que cuenta con la experiencia y la responsabilidad de desarrollar y adoptar políticas y procedimientos de ciberseguridad para la infraestructura del laboratorio y los sistemas del edificio
  - C. confiar en los proveedores, quienes son responsables de garantizar que sus sistemas, equipos y personal de servicio estén libres de vulnerabilidades y cumplan con las mejores prácticas de ciberseguridad
  - D. colaborar con los gerentes del laboratorio para realizar un escaneo de vulnerabilidades y una prueba de penetración de los sistemas de contención del edificio al menos una vez al mes
5. Complete la siguiente afirmación: Al desarrollar un plan de respuesta ante incidentes de ciberseguridad para su laboratorio biológico, una organización debe \_\_\_\_\_.
- A. prepararse y desarrollar instrucciones paso a paso para que todos los empleados manejen cada posible incidente que pudiera impactar negativamente a la organización
  - B. enfocarse en estar preparada de forma general en toda la organización, con mayor énfasis en cómo manejar incidentes que utilicen vectores de ataque comunes\*
  - C. limitar estrictamente el intercambio de información sobre todos los aspectos del plan dentro de la organización para reducir la probabilidad de ciberataques internos
  - D. establecer procedimientos escritos para manejar múltiples incidentes en orden de llegada, con el fin de ahorrar tiempo al personal encargado de la respuesta

## *Referencias*

Además del conocimiento de la terminología básica y los fundamentos de la ciberseguridad, se sugiere que la preparación para el examen incluya, entre otros, los siguientes 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.