

Reglamento Oficial: CyberChallenge 2026 CENFOTEC

Fecha del evento: 8 de agosto de 2026

Horario de competencia: 9:00 AM a 1:00 PM (4 horas)

Modalidad: Jeopardy por Equipos (Máximo 3 integrantes)

El presente documento establece las normas, lineamientos y código de conducta obligatorios para todos los participantes del CyberChallenge 2026 CENFOTEC. Al ser un evento diseñado para estudiantes de nivel principiante, el objetivo principal es el aprendizaje práctico, la resolución de problemas y el desarrollo de habilidades analíticas en ciberseguridad bajo un entorno de competencia justo y controlado.

1. Dinámica de la Competencia y Puntuación

- **Formato Jeopardy:** La competencia consta de una serie de retos independientes divididos en diversas categorías (Criptografía, Forense, Web y OSINT). Cada reto resuelto otorgará una cantidad fija de puntos.
- **Puntuación Estática:** El valor de los retos no disminuirá con la cantidad de resoluciones. Todos los desafíos mantienen su puntaje inicial de principio a fin del evento.
- **Criterio de Desempate:** En caso de que dos o más equipos finalicen la competencia con la misma cantidad de puntos, la plataforma de manera automatizada otorgará la posición superior al equipo que haya alcanzado dicha puntuación en el menor tiempo.

2. Uso de Teléfonos Celulares y Dispositivos Móviles

- **Restricción de Comunicación:** Queda estrictamente prohibido utilizar teléfonos celulares, aplicaciones de mensajería instantánea (WhatsApp, Telegram, etc.) o redes sociales para transferir soluciones, metodologías, banderas (flags) o capturas de pantalla a miembros de otros equipos competidores.

3. Prohibición Absoluta de Inteligencia Artificial (No IA)

- **Cero Tolerancia:** Está terminantemente prohibido el uso de herramientas, modelos o asistentes basados en Inteligencia Artificial (incluyendo, pero no limitado a: ChatGPT, Claude, Gemini, Microsoft Copilot o similares) durante el desarrollo de las 4 horas de competencia.
- **Filosofía Educativa:** El valor del CTF radica en el esfuerzo analítico e investigativo del estudiante. El uso de herramientas de generación automática de código o resolución de acertijos destruye el proceso pedagógico.
- **Penalización Extrema:** Cualquier equipo que sea detectado utilizando o consultando herramientas de Inteligencia Artificial para decodificar textos, analizar código fuente o extraer banderas será sancionado con la **descalificación inmediata e irrevocable** de

todo el evento, perdiendo cualquier derecho a premiación.

4. Sistema de Pistas (Hints) y Herramientas Permitidas

- **Pistas Accesibles y Gratuitas:** Con el fin de evitar la frustración y guiar el aprendizaje de los novatos, todos los retos cuentan con pistas habilitadas en la plataforma CTFd. **El uso de estas pistas es 100% gratuito y restará 1 punto al equipo.**
- **Software Autorizado:** Se fomenta el uso de utilidades y plataformas web públicas de código abierto sugeridas en las pistas, tales como: CyberChef, decodificadores Rot13, analizadores de metadatos EXIF en línea y el software de audio gratuito Audacity.

5. Juego Limpio (Fair Play) y Seguridad de la Infraestructura

- **Protección del Servidor:** La competencia corre sobre una infraestructura virtual en la nube (Hostinger VPS) dimensionada específicamente para soportar las peticiones del evento de forma fluida. Queda prohibido el uso de herramientas de escaneo automatizado masivo o agresivo (como fuerza bruta destructiva mediante utilidades como dirb o gobuster).
- **Prohibición de Ataques de Infraestructura:** Cualquier intento de lanzar ataques de Denegación de Servicio (DoS/DDoS) contra el servidor del CTF o a alguno de los equipos, sabotear los contenedores de los retos, alterar el código de la plataforma o manipular el puntaje ajeno resultará en la expulsión inmediata del evento y se reportará a las autoridades académicas correspondientes.