

HackHowl

cuyo propósito es inspirar a los participantes a mejorar continuamente sus habilidades en el hacking ético, motivándolos a adquirir nuevas técnicas y conocimientos mediante actividades como Capture The Flag (CTF) y un programa de Bug Bounty con un enfoque educativo. Esta experiencia es esencial para prepararlos para los trabajos en su área, como pentesting y ciberseguridad, donde podrán desarrollar y aplicar conocimientos abordando desafíos más avanzados, de acuerdo con las siguientes bases de participación:

PRIMERA: Comité organizador

- El comité organizador está conformado por especialistas de ciberseguridad de Maikron y miembros del capítulo estudiantil AAAiMX.

SEGUNDA: Participantes

- Podrán participar profesionales, aficionados y estudiantes en las áreas de tecnologías.
- Los equipos deberán estar conformados por **mínimo tres y máximo cinco participantes**.
- Cualquier modificación en los participantes debe notificarse a más tardar el 31 de mayo al correo: hackhowl@maikron.org.
- Los nombres de los equipos serán revisados por el comité organizador.

TERCERA: Proceso de registro

- El proceso de registro se realizará a través de la plataforma EventBrite (<https://www.eventbrite.com.mx/e/882388857827>).
- Durante las dos primeras etapas del evento (7 y 8 de junio) el evento consistirá de dos turnos: matutino (9:00-13:00 hrs.) y vespertino (15:00-19:00 hrs.). Cada equipo elegirá el turno de su preferencia durante el proceso de registro.
- Se tomarán en cuenta los primeros 80 equipos registrados (40 por cada cupo) a nivel nacional y se enviará un correo de verificación al representante del equipo.
- La cuota de inscripción al evento tiene un costo de \$420 MXN **por equipo**.

CUARTA: Fechas

- El registro estará abierto a partir de la publicación de la presente convocatoria y hasta el **31 de mayo de 2024** o hasta registrarse el máximo de equipos permitidos.
- El evento se celebrará los días **7, 8 y 9** de junio del presente año. Los días 7 y 8 de junio en los horarios mencionados en la tercera base, y el día 9 de junio en horario de 12:00 a 18:00 hrs.

QUINTA: Dinámica del evento

- El día 7 de junio, la primera etapa del evento, consistirá en un evento CTF.
- El objetivo del CTF es encontrar el mayor número de *flags*. Las diversas *flags* existentes tienen puntajes diferentes, las cuales varían según su nivel de dificultad.
 - Fácil: 150 puntos
 - Intermedio: 350 puntos.
 - Avanzado: 550 puntos.
 - Algunas banderas podrían pedir la subida de evidencia mediante capturas de pantalla.
- Los días 8 y 9 de junio, las segunda y tercera etapas del evento, respectivamente, consistirán en un evento Bug Bounty.
- El objetivo del Bug Bounty es que los equipos logren encontrar vulnerabilidades en un entorno en producción. Se premiará al equipo que encuentre vulnerabilidades, que las logre explotar y que documente adecuadamente sus hallazgos.

SEXTA: Competencia

ETAPA 1

- Los equipos que coloquen primero sus banderas y/o respuestas serán los que estén adelante en el marcador.
- En caso de empate, se considerará en delantera al equipo que consiga el puntaje en el **menor tiempo**.
- Esta etapa se llevará a cabo en el turno que hayan elegido los equipos durante el proceso de registro.
- Solo los equipos mejor puntuados avanzarán a la siguiente etapa, a criterio del comité organizador, que no excederá del 50% de los equipos registrados.

ETAPA 2

- Durante esta etapa del Bug Bounty, se proporcionará a

cada equipo un formato de referencia para reportar errores o vulnerabilidades.

- Esta etapa se llevará a cabo en el turno que hayan elegido los equipos durante el proceso de registro.
- Los puntos otorgados serán con base en los errores o vulnerabilidades reportadas en el formato.
- Solo los equipos mejor puntuados avanzarán a la siguiente etapa, a criterio del comité organizador, que no excederá del 25% de los equipos registrados.

ETAPA 3

- Durante esta última etapa, se proporcionarán formatos complementarios al anterior.
- Se evaluará la explotación de vulnerabilidades, la documentación de evidencia y las recomendaciones para solucionar estos problemas.
- Se evaluará también el contenido del documento y su calidad.
- Especialistas en ciberseguridad realizarán la evaluación de los documentos y otorgarán los puntos finales a los equipos.
- El equipo con la puntuación más alta, según la tabla de marcador, podrá ser considerado como ganador.
- Las posiciones se determinarán con base en el posicionamiento de los equipos en el marcador.
- La tercera y última etapa se llevará a cabo en un horario único para todos los equipos: de 12:00 a 18:00 hrs.

SÉPTIMA: Desarrollo

- Se podrá utilizar cualquier sistema operativo; recomendación: Kali Linux.
- El evento se llevará a cabo en línea (no habrá modalidad presencial) y cada participante deberá contar con sus propios recursos, como equipos de computación y acceso a internet, para participar en línea.
- Únicamente se contarán los desafíos que se encuentren el día del evento. Específicamente, ese día se revelará cuál será el desafío.
- Están estrictamente prohibidas las siguientes acciones:
 - Compartir las respuestas o banderas a otro equipo.
 - Cooperar con otro equipo para la resolución de los desafíos.
 - Acceder dentro de la máquina virtual desde las opciones del virtualizador que se haya elegido. (En caso de sospecha, se pedirá replicar la resolución del desafío).
 - Compartir hallazgos de la documentación a otros equipos.
 - Cualquier otra acción que atente en contra del desarrollo ético de la competencia, a criterio del comité organizador.
 - En caso de incumplimiento de alguna de estas reglas, el equipo o equipos involucrados serán descalificados del evento sin reintegro de la cuota de inscripción.

OCTAVA: Premiación

- La notificación de los ganadores se comunicará a más tardar el 14 de junio a través de los canales oficiales y mediante correo electrónico al representante del equipo.
- Los premios consistirán en tarjetas de regalo y suscripciones a plataformas educativas de ciberseguridad.
- Los premios serán entregados directamente al representante del equipo ganador.
- Se otorgarán certificados de participación a todos los integrantes de los equipos participantes.

NOVENA: Casos imprevistos

- Cualquier caso imprevisto será atendido por el comité organizador.